

Cisco Stealthwatch SaaS Test Drive Labs

Welcome to the Cisco Stealthwatch SaaS dCloud (Demo Cloud) Test Drive Labs! You will learn how to turn your network into a security sensor. Stealthwatch Cloud consists of two products, Private Network Monitoring (PNM) and Public Cloud Monitoring (PCM). This lab focuses on PNM use-cases, the lecture prior to the lab covers cloud monitoring topics. As part of this lab, you get hands on access to a pre-configured network with traffic that you generate to test live use cases including:

- Breach Detection
- Insider and Advanced Threat Detection
- High Risk Application Detection
- Policy Violations
- Encrypted Traffic Analytics

This lab lets you play the role of an attacker generating traffic; then you log into Stealthwatch Cloud as a defender to learn how to see and respond to these attacks. Completing these labs will help provide test plans to effectively use and operationalize Stealthwatch Cloud. Everything learned in these labs can be carried over into a production deployment of Stealthwatch.

Table of Contents

Requirements	3
About This Test Drive Lab.....	3
Topology & Accounts	3
<i>Accounts and Passwords for this dCloud Lab</i>	5
<i>Getting Started.....</i>	6
<i>Validating Your Workstation 1 - ipconfig</i>	7
<i>Access your Stealthwatch Cloud Account.....</i>	8
Initial setup of Stealthwatch Cloud.....	10
<i>Download scripts using GitBash</i>	11
<i>Configure UDP Director.....</i>	12
<i>Configure Stealthwatch Cloud Sensor.....</i>	14
Initial Stealthwatch Cloud Portal Configuration	18
<i>Configure public subnet used in Dcloud in your SWC portal.</i>	18
<i>Configure a TOR Watchlist in the Stealthwatch Cloud portal</i>	20
<i>Sensor NetFlow Collection</i>	22

Workstation Setup and Portal Overview	26
<i>Validating Your Workstation 1 – Install Tor Browser</i>	26
<i>Validating Your Workstation 1 - netstat</i>	27
<i>Configure Country Watchlists in the Stealthwatch Cloud portal</i>	28
<i>Stealthwatch Cloud – Flow Search</i>	29
<i>Finding Flows using Session Filter</i>	35
<i>Finding Flows for the TOR download</i>	37
<i>Summary</i>	39
Breach Detection.....	40
Lab 1: Remote Access Breach using stolen credentials.....	41
<i>Business Objectives</i>	41
<i>Test Drive Objectives</i>	41
<i>Test Drive Requirements</i>	41
<i>Test Drive Outline</i>	42
<i>Summary</i>	56
Lab 2: Historical Traffic Analysis to Identify Threats from Suspect Countries	56
<i>Business Objectives</i>	56
<i>Test Drive Objectives</i>	56
<i>Test Drive Requirements</i>	56
<i>Test Drive Outline</i>	57
<i>Summary</i>	64
Insider & Advanced Threat Detection	65
Lab 3: Data Exfiltration	65
<i>Business Objective</i>	65
<i>Test Drive Objectives</i>	66
<i>Test Drive Requirements</i>	66
<i>Test Drive Outline</i>	66
High Risk Application Detection	70
Lab 4: Detecting Internal Telnet Traffic	70
<i>Business Objective</i>	70
<i>Test Drive Objective</i>	70
<i>Test Drive Requirements</i>	70
<i>Test Drive Outline</i>	70
<i>Summary</i>	78
Encrypted Traffic Analytics (ETA)	79
<i>Business Objectives</i>	79
<i>Requirements</i>	79
<i>Review Vulnerable Transport Alert</i>	80
<i>Crypto audit to enforce authorized encryption standards</i>	81
<i>Review Encrypted Traffic Query</i>	81
Appendix	83

Understanding NetFlow & IPFIX.....	83
<i>Business Objectives</i>	83
<i>Test Drive Objectives</i>	83
<i>Test Drive Requirements</i>	83
<i>Test Drive Outline</i>	83
Lab: Understanding NetFlow.....	84
Steps to enable flow	86
<i>Reviewing a NetFlow Packet Capture</i>	90
<i>Summary</i>	92

Requirements

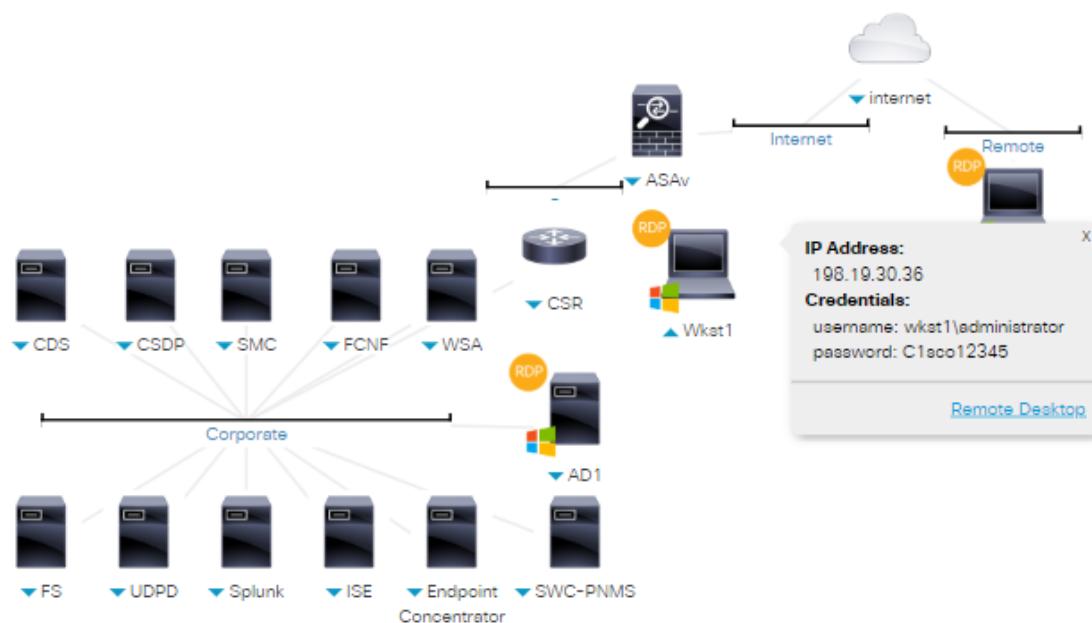
1. Laptop with network capabilities
2. A Cisco.com account (go here to [Register](#) if you need one)
3. A Stealthwatch Cloud Portal (provided by lab proctor)

About This Test Drive Lab

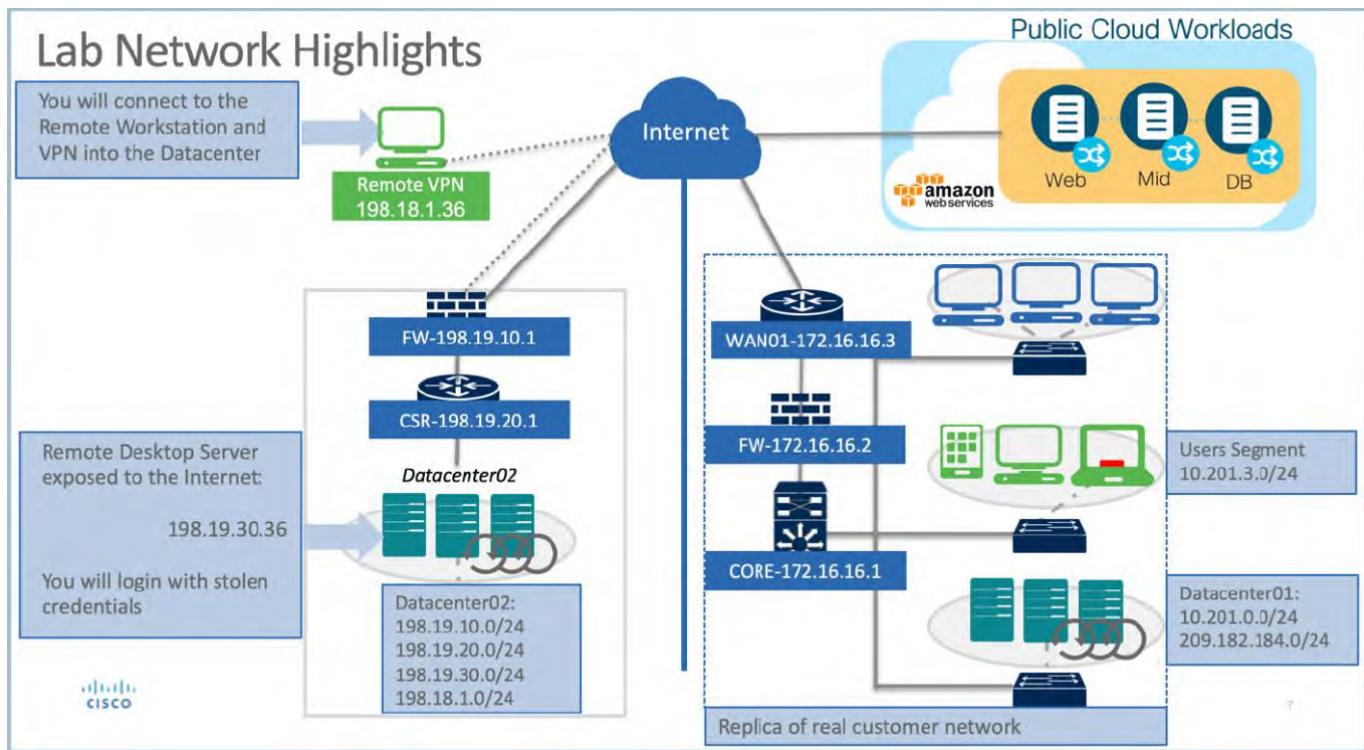
The Cisco Stealthwatch Cloud Test Drive has been built as a training platform to gain first-hand experience using Stealthwatch Cloud SaaS. Students get to experience life-like cyber security attack situations in a virtualized enterprise lab environment, playing the role of an attacker and defender. Using an environment similar to many enterprise networks, students will learn and understand how their own environments get compromised, how security breaches get detected, and how to respond using Stealthwatch.

Topology & Accounts

This lab includes preconfigured users and components to illustrate scripted scenarios and features of Cisco Stealthwatch Cloud. Most components are fully configurable with predefined administrative user accounts. You can see the IP addresses and user account credentials to access a component by clicking on their icon in the Topology menu.

Figure 1. dCloud Topology

This lab includes preconfigured components such as ASA Firewalls, Cloud Services Routers, etc. Figure 2 highlights how the demo environment is setup. The majority of the exercises are done using Wkst1 via remote desktop.

Figure 2. Lab Setup

Accounts and Passwords for this dCloud Lab

Figure 3. Credentials

Username	Password	Endpoint Devices	IP Address
wkst1\Administrator	C1sco12345	Workstation1	198.19.30.36
admin	C1sco12345	Management Console	198.19.20.136
admin	C1sco12345	Flow Collector	198.19.20.137
admin	C1sco12345	Flow Sensor	198.19.20.138
admin	C1sco12345	UDP Director	198.19.20.139
admin	C1sco12345	Remote Workstation	198.18.1.36
admin	C1sco12345	Splunk	198.19.20.140
root	C1sco12345	CDS	198.19.20.134
admin	C1sco12345	CSR	198.19.10.2, 198.19.20.1, 198.19.30.1
admin	C1sco12345	ASAv	198.19.10.1, 198.18.133.100
dcloud\administrator	C1sco12345	AD1	198.19.20.10
admin	C1sco12345	WSA	198.19.20.51
admin	C1sco12345	ISE	198.19.20.141
admin	C1sco12345	Endpoint Concentrator	198.19.20.142
swcadmin	C1sco12345	SWC Sensor	198.19.20.143

Getting Started

This lab allows you to familiarize yourself with dCloud. It walks through connecting to your shared session, validating the machine you will be connecting to in the data center and ensuring that Stealthwatch Cloud is up and available.

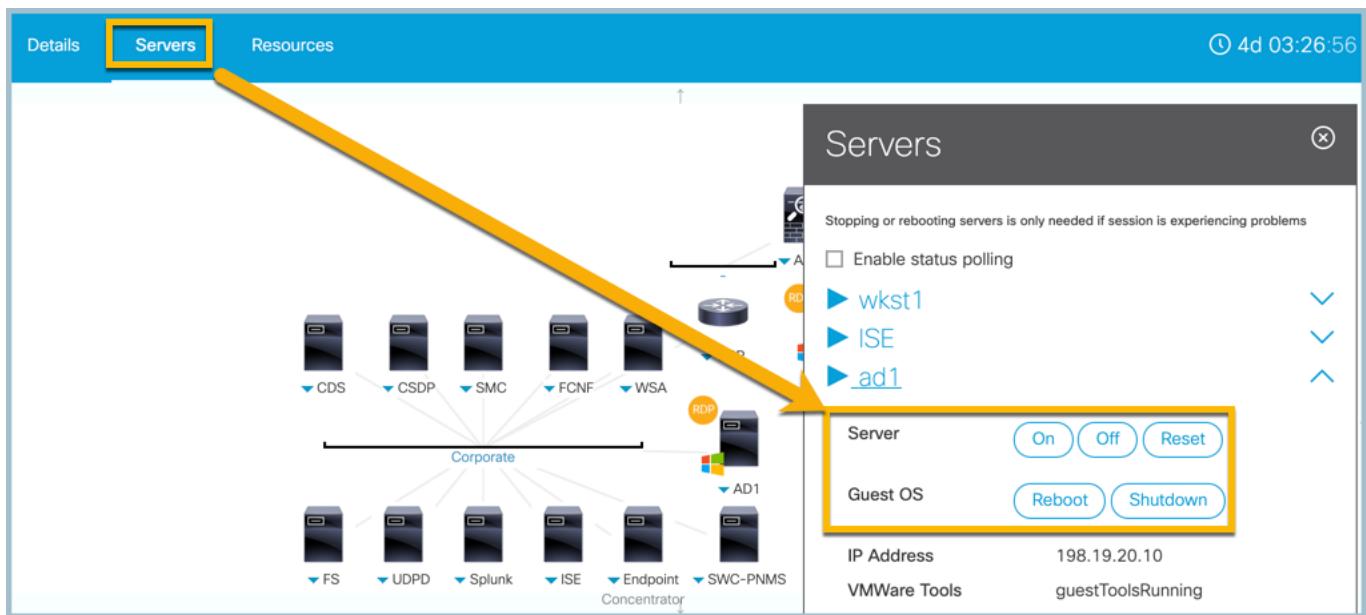
Let's begin.

1. Login using your Cisco.com account to <https://dcloud.cisco.com>
2. Select **My Hub**, shown below. If you do not see an active session you may need to change to a different dCloud data center location. This is done by clicking the green circle in the upper right window. As your proctor which data center the lab is located in.
3. Select **View** for Test Drive: Cisco Network as an Enhanced Sensor with Stealthwatch, ETA and ISE Lab v1.1 session, shown below.

Figure 4. dCloud Session

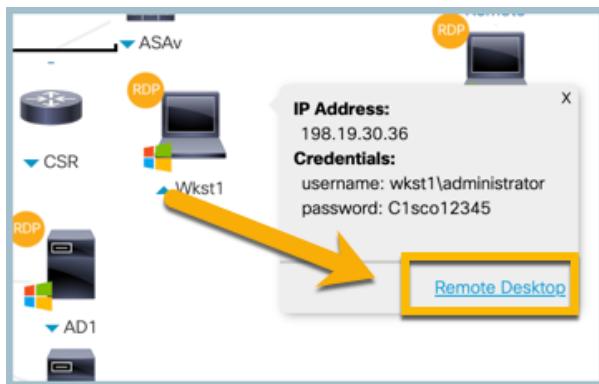
4. Select **Servers** to view the servers running for this lab.
5. The **Servers** tab pulls up all of the systems running with the lab environment. You have the ability to reboot the platforms from this location (e.g. reboot your windows workstation).

Figure 5. dCloud Services



- To work within this lab, you will need to access Wkst1, which gives you access to all data center resources. Click **Remote Desktop** link to launch a web Remote Desktop session built within dCloud shown below.

Figure 6. Workstation1 Remote Desktop



Validating Your Workstation 1 – ipconfig

Workstation 1 will be the Workstation you use. Let's validate the IP address of your Workstation 1. Refer to the figure below.

- From the Workstation 1 click **Start** and type **cmd** in the search box.
- Click **cmd.exe** from the search result.
- Type **ipconfig** and hit enter.

- Validate the IP address of your Workstation 1 is **198.19.30.36**. Make note of this IP address because you will use it in most labs.

Figure 7. Validate IP address of Workstation 1

```

Administrator: cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32\ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::6da3:bcc4:eaec:a2f7%16
  Autoconfiguration IPv4 Address. . . : 169.254.162.247
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . :

Ethernet adapter Npcap Loopback Adapter:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::95e:532b:129b:659c%15
  Autoconfiguration IPv4 Address. . . : 169.254.101.156
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . :

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix  . :
  IPv4 Address. . . . . : 198.19.30.36
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 198.19.30.1

Tunnel adapter isatap.{073BCF95-D7DF-457E-9ACB-560C80D217B2}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

Tunnel adapter 6T04 Adapter:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

```

Access your Stealthwatch Cloud Account

As part of this Test Drive a new Stealthwatch Cloud portal was created. You will either have an invitation to the email attached to your CCO ID or the proctor will assign you a login at the beginning of the session.

The email will be from service@obsvrbl.com. It will contain a onetime URL for creating your credentials. Additionally, since the portal is created unique to this Test Drive you will be attaching the Stealthwatch cloud virtual appliance (Flow Collector) in Dcloud to your cloud portal as well as some initial portal configurations.

Figure 8. Stealthwatch Cloud user registration

The screenshot shows the 'Stealthwatch Cloud' user registration interface. At the top left is the Cisco logo. To its right, the text 'Stealthwatch Cloud' is displayed. Below this, a grey header bar contains the text 'Welcome to Stealthwatch Cloud'. Underneath the header, a message states: 'john.heintz@obsvrbl.com has invited you to join cisco-johheintz.obsvrbl.com. Before you can get started, you will need to set up your Cisco Secure Sign-On account. Once your account has been set up, you will be able to access your Stealthwatch Cloud portal.' A prominent blue button labeled 'Set Up My Account' is centered below the message. A small note below the button says 'This link expires in 7 days'. At the bottom of the page, a section titled 'With Cisco Secure Sign-On, you'll have:' lists several features:

- **Strong and resilient identity:** Security that meets the highest industry standards, including AICPA SOC 2, CSA-Star, and ISO 27001. It also supports segregated FedRAMP and HIPAA environments for customers.
- **Duo Multi-Factor Authentication (MFA):** Duo MFA integrated with Cisco Secure Sign-On means adaptive, layered, and simplified authentication. One push notification, one tap, instant access.
- **A single sign-in for seamless workflows:** Enter a single username and password to access all your applications, anywhere, and on any device, while maintaining context through workflows.
- **A customized experience:** Arrange your work apps on your Cisco Secure Sign-On dashboard any way you want. Tabs and a search bar help keep you organized.

1. Register credentials using the link provided in the email
2. Login to the portal with the recently created credentials

Figure 9. New portal setup page

Welcome to Stealthwatch Cloud!

Take these steps to ensure a smooth experience:

- Verify that your sensors are connecting to our infrastructure and sending data. The  icon on top of this page shows the status of your sensors.
- Site managers can invite users to the portal from the settings page.
- Sensor placement and mirror port configuration impact our visibility into your network.
- Visit the [FAQ](#) for answers to common questions.
- Don't hesitate to contact support if you have any further questions.

We are actively monitoring your network for abnormal activity. Keep in mind that some alerts require **30 days** of network history, while others are active immediately. Read about the alerts and observations that are monitoring your network.



Gathering Data | 0 of 30 days gathered

Welcome to Stealthwatch Cloud

On-premises network

To start monitoring a network that you manage, you'll need to install a sensor.

Begin by downloading the sensor image:

 [ona-18.04.3-server-amd64.iso](#)

SHA-256:
214ffd997c24009c9365cb40da51e17d0bacc64e614f3a605612cfda0e4ec3c

Our sensor image includes the Ubuntu Linux distribution and other free software licensed under the terms of the GNU General Public License and other open source licenses.

- To learn more about Ubuntu, see the [Ubuntu website](#).
- To access source code and license notices for the open source in our software, see our [Github repository](#).
- For complete information on all of the open source software used please use [this link](#).

After you've downloaded the sensor image, install it on a machine. See the [installation guide for instructions](#).

Enter the public IP address your sensor will use when sending data.

Public IP:

Cloud network

AWS Virtual Private Cloud (VPC)

To start monitoring an AWS Virtual Private Cloud (VPC), you'll need to set up VPC Flow Logs. For step-by-step instructions, see the [VPC Flow Logs instructions](#).

Google Cloud Platform VPC Flow Logs

To monitor a Google Cloud Platform network, you'll need to set up a service account with log viewing access. Refer to the [GCP integration page](#) for detailed instructions.

Microsoft Azure NSG Flow Logs v2

To monitor a Microsoft Azure network, you'll need to set up an application to read data and NSG Flow Logs v2. See the [Azure integration page](#) for instructions.

Initial setup of Stealthwatch Cloud

This lab uses a new Stealthwatch Cloud portal, as such we will be performing some initial steps to:

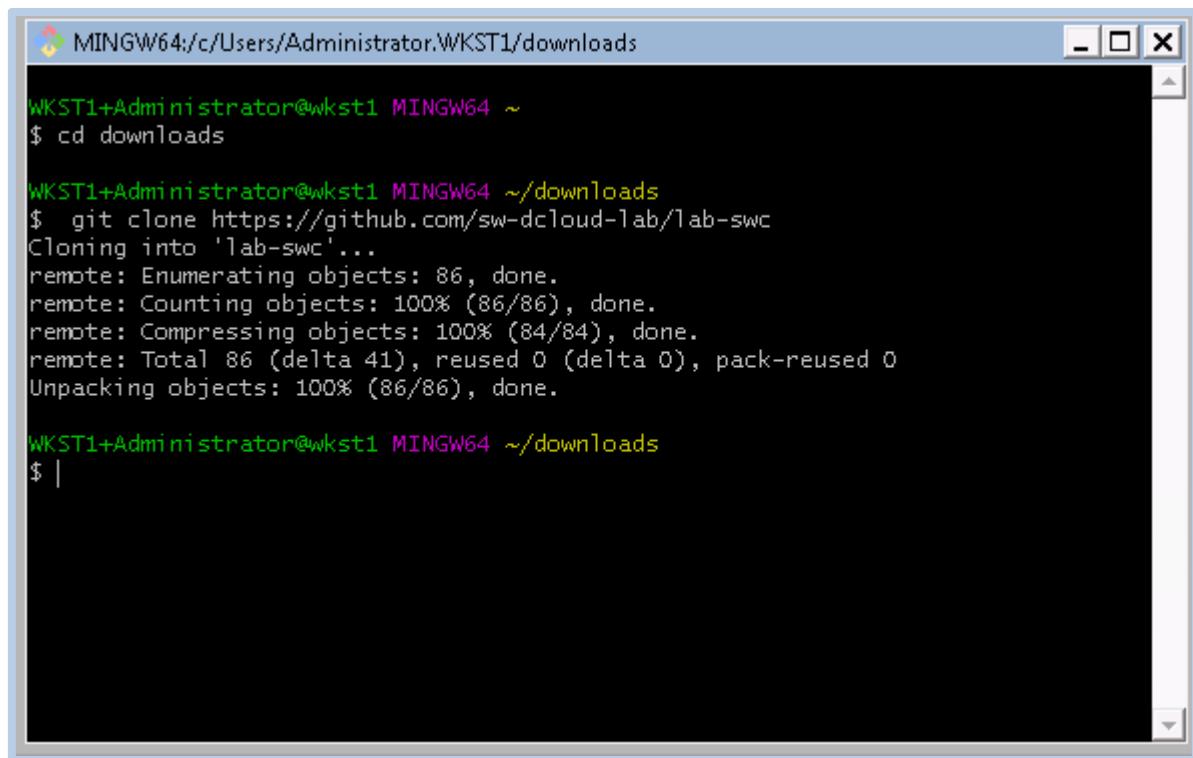
1. Use Gitbash to download scripts to the local machine for easier copy/paste operations
2. Forward NetFlow from the UDP Director to the Stealthwatch Cloud Sensor

3. Link the sensor the cloud portal and configure for enhanced NetFlow
4. Set some initial configurations in the portal.

Download scripts using GitBash

To make the lab easier we are hosting some of the scripts on GitHub, we will be using GitBash to download them to the local workstation.

Figure 10. GitBash



```
MINGW64:/c/Users/Administrator.WKST1/downloads
WKST1+Administrator@wkst1 MINGW64 ~
$ cd downloads

WKST1+Administrator@wkst1 MINGW64 ~/downloads
$ git clone https://github.com/sw-dcloud-lab/lab-swc
Cloning into 'lab-swc'...
remote: Enumerating objects: 86, done.
remote: Counting objects: 100% (86/86), done.
remote: Compressing objects: 100% (84/84), done.
remote: Total 86 (delta 41), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (86/86), done.

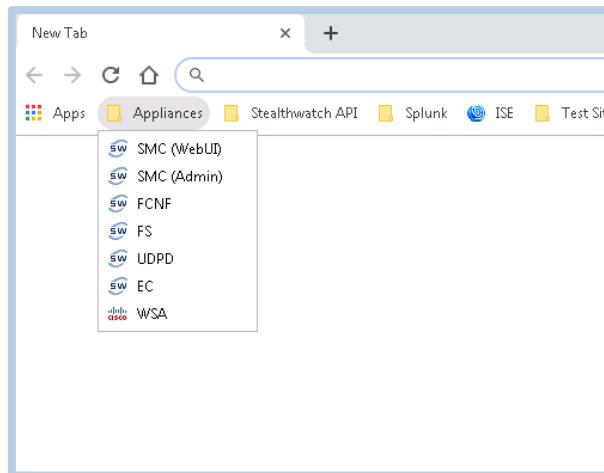
WKST1+Administrator@wkst1 MINGW64 ~/downloads
$ |
```

1. Open [GitBash](#) from desktop of Wkst1
2. Change directory to Downloads `cd downloads`
3. Type [`git clone https://github.com/sw-dcloud-lab/lab-swc`](https://github.com/sw-dcloud-lab/lab-swc) to sync files to the workstation.
This will copy files to the /downloads directory on the workstation and put them in the lab-swc folder.
4. Open downloads to confirm you have the lab-swc directory.

Configure UDP Director

1. Open the Chrome browser in Wkst1
2. Select SMC (WebUI) under Appliances, if you get a security warning click advanced then proceed to 198.19.20.136. User is admin, password is C1sco12345

Figure 11. Location of SMC



3. We need to configure the UDP Director to forward flows to the Stealthwatch Cloud virtual appliance. Start by selecting **UDP Director Configuration** under the settings icon.
4. Next select **Configure Forwarding Rules**, this is listed under the Actions menu.

Figure 12. UDP Director Selection in SMC

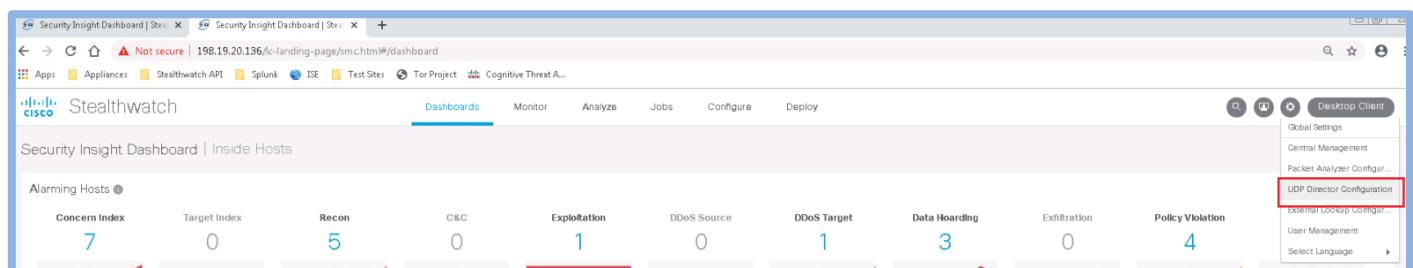


Figure 13. Configure Forwarding Rules

The screenshot shows the Stealthwatch UDP Director Configuration interface. At the top, there are tabs for Dashboards, Monitor, Analyze, Jobs, Configure, and Deploy. Below the tabs, it says "UDP Directors" and lists one device: "UDPD" with IP "198.19.20.139". The "Management Channel Status" indicates "Last Seen : 12:03 PM 12/06/2019". On the right, there are three actions: "Configure Forwarding Rules" (highlighted with a red box), "Configure High Availability", and "Export Forwarding Rules".

- Select **Import/Export**, then **Import Rules**, select the XML file downloaded earlier using GitBash (downloads/lab-swc/UDPD-fwd-rules.xml). **Note:** Select **Sync** to save changes. The UDP Director is a Stealthwatch product for forwarding flows, in this lab we have multiple devices that need the flows, so we are using this to share the flows.

Figure 14. UDP Director Forwarding Rules

The screenshot shows the "Forwarding Rules | UDPD - 198.19.20.139" configuration page. It displays a table with six rows of forwarding rules. The columns are: RULE, DESCRIPTION, SOURCE IP ADDRESS & PORT LIST, DESTINATION IP ADDRESS, DESTINATION PORT NUMBER, and Actions. The "Import/Export" button at the top right is highlighted with a red box. The rules are:

RULE	DESCRIPTION	SOURCE IP ADDRESS & PORT LIST	DESTINATION IP ADDRESS	DESTINATION PORT NUMBER
1	Syslog from WSA to CSDP	198.19.20.51:514	198.19.20.136	514
2	Syslog to SMC	All:514	198.19.20.136	514
3	Syslog from WSA to FC	198.19.20.51:514	198.19.20.137	514
4	NetFlow to FCNF	All:2055	198.19.20.137	2055
5	AnyConnect NVM Flows to EC	All:2056	198.19.20.142	2056
6	UDP Director to SWC Sensor	All:2055	198.19.20.143	2055

Figure 15. UDP Director Forwarding Rules after import

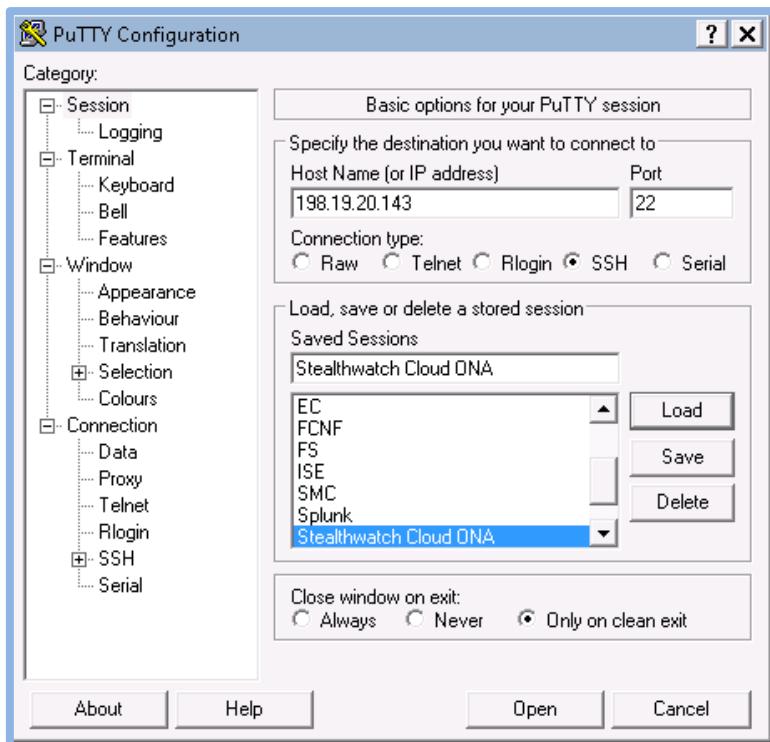
RULE	DESCRIPTION	SOURCE IP ADDRESS & PORT LIST	DESTINATION IP ADDRESS	DESTINATION PORT NUMBER	ACTION:
1	Syslog from WSA to CSDP	198.19.20.51:514	198.19.20.135	514	
2	Syslog to SMC	All:514	198.19.20.136	514	
3	Syslog from WSA to FC	198.19.20.51:514	198.19.20.137	514	
4	NetFlow to FCNF	All:2055	198.19.20.137	2055	
5	AnyConnect NVM Flows to EC	All:2056	198.19.20.142	2056	
6	UDPD ASA to SWC Sensor	198.19.10.1:2055 172.16.16.2:2055	198.19.20.143	9997	
7	UDPD Netflow v9 to SWC Sensor	172.16.16.1:2055 172.16.16.3:2055 172.16.16.50:2055 172.16.16.100:2055 172.16.16.200:2055 198.18.128.138:2055 198.19.20.135:2055	198.19.20.143	9995	
8	UDPD ETA flow to SWC Sensor	198.19.20.1:2055	198.19.20.143	2055	
9	UDPD IPFIX to SWC Sensor	198.19.20.138:2055 198.19.20.142:2055	198.19.20.143	4739	

Configure Stealthwatch Cloud Sensor

In this next session we are going to setup the Stealthwatch Cloud sensor. Normally we would link a sensor to a cloud portal by finding the public IP address it is using to access the internet and entering it into the portal. However, dCloud shares public IP space we cannot use this method. This means more CLI fun for you as will be using the key for your portal to manually link the sensor.

Best Practice – Open your Stealthwatch Cloud portal inside the browser of Wkst1 so that you can copy/paste the key.

1. Next, we are going to configure some settings directly on the Stealthwatch Cloud virtual appliance. Open the swc_sensor_commands text file, this is a document we synced using GitBash earlier, it is located in /downloads/lab-swc. It contains the commands you can copy/paste that are referenced below.

Figure 16. Putty Window

2. Open Putty on Wkst1
3. Select StealthWatch Cloud ONA
Login as **swcadmin**, password is **C1sco12345**
4. Enter the first command after the # statement (, this will switch you to Super User and stop the Stealthwatch Cloud service. You will be prompted for your password again.

Figure 17. Stealthwatch Cloud CLI

```

#run this command first to stop the service and switch to super user
sudo service obsrvbl-on-a stop

#run these command to delete the stale files
sudo rm -rf /opt/obsrvb1-on-a/logs/1pf1x/
sudo mkdir /opt/obsrvb1-on-a/logs/1pf1x/
sudo chown obsrvbl_ona: /opt/obsrvb1-on-a/logs/1pf1x/
sudo rm -rf /opt/obsrvb1-on-a/logs/pna/
sudo mkdir /opt/obsrvb1-on-a/logs/pna/
sudo chown obsrvbl_ona: /opt/obsrvb1-on-a/logs/pna/

# Run this command to edit the local config file and add your portal key.
sudo rm /opt/obsrvb1-on-a/config.auto
sudo nano /opt/obsrvb1-on-a/config.local

# This is the string to add to config.local, add it at the end of the file, replace OBSRVBL_SERVICE_KEY="xxxxxx"
OBSRVBL_SERVICE_KEY="xxxxxx"

# once the key has been added, save the file (Ctrl + X) and then start the se
sudo service obsrvbl-on-a start

[swcadmin@centos ~]$ sudo service obsrvbl-on-a stop
[sudo] password for swcadmin:
Redirecting to /bin/systemctl stop obsrvbl-on-a.service
[swcadmin@centos ~]$ 

```

- These next group of commands instructs the OS to remove any stale flow data files. Once a sensor is booted, the Stealthwatch Cloud service automatically starts collecting network data and queues that data until it connects to a portal. In this case, we want to remove the old data and start fresh with our test drive. These commands are located in the “swc_sensor_commands.txt” document.

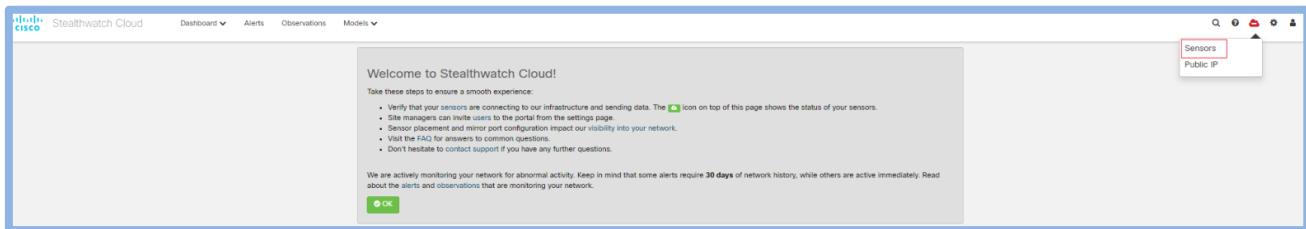
```

sudo rm -rf /opt/obsvbl-ona/logs/ipfix/
sudo mkdir /opt/obsvbl-ona/logs/ipfix/
sudo chown obsvbl_ona: /opt/obsvbl-ona/logs/ipfix/
sudo rm -rf /opt/obsvbl-ona/logs/pna/
sudo mkdir /opt/obsvbl-ona/logs/pna/
sudo chown obsvbl_ona: /opt/obsvbl-ona/logs/pna/

```

- Next we be attaching the sensor to your portal. Since Dcloud re-uses the public IP space, we cannot use the normal method of using your public IP address. To work around this limitation, we will need to edit a config file on the sensor and manually add the key from your portal. The command for this is located in the “swc_sensor_commands.txt” file.
 - Login to your Stealthwatch Cloud Portal
 - In the upper left, select the **cloud icon**
 - Select **Sensors**

Figure 18. Service Key Location



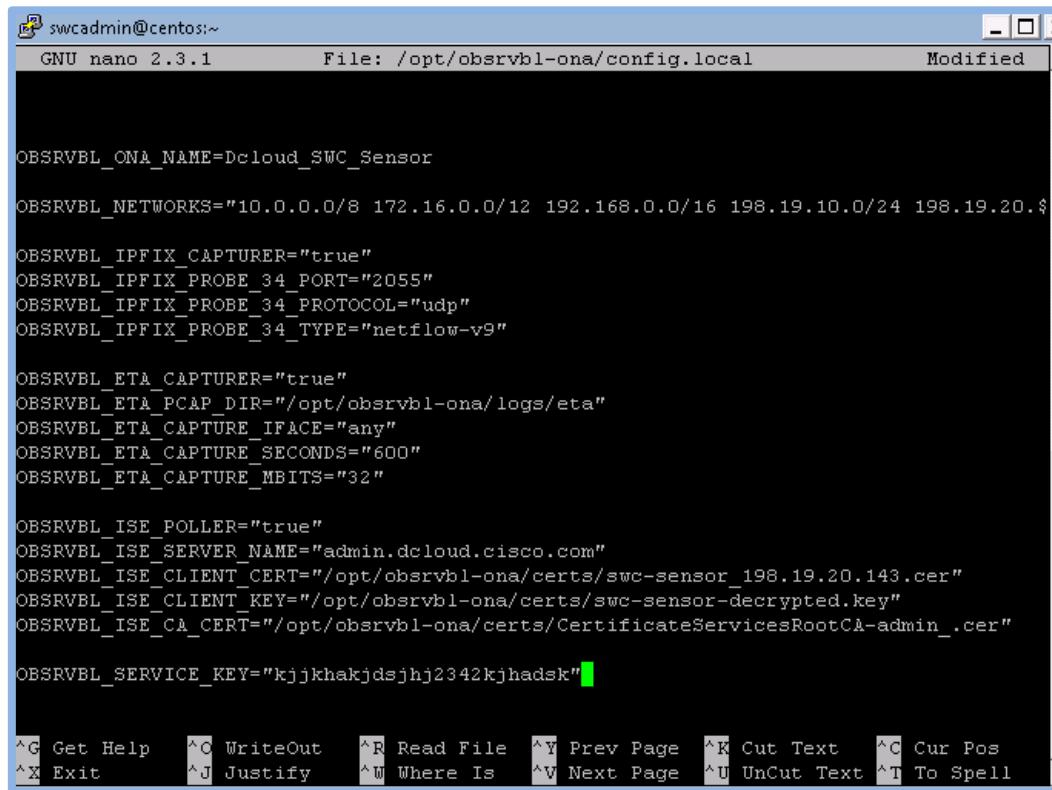
- Scroll down to the bottom, copy the service key to the swc_sensor_commands.txt file. Use the line that starts with “OBSRVBL_SERVICE_KEY=

- e. Be sure to add quotes to the beginning and end of the key string. When finished it should look like figure 19.
- f. Run the series of commands in the swc_sensor_commands.txt file that are for editing the local config file and adding the portal key. This will edit a file called config.local. You will paste the service key into this file (location doesn't matter). After finished it should look like figure 20.
- g. Hold **Control + O** to save, hit enter at save location prompt
- h. Hold **Control + X** to exit
- i. Run the last command in the swc_sensor_commands.txt to restart the Stealthwatch service

Figure 19. Service Key in the text file

```
# This is the string to add to config.local, add it at the end of the file, replace xxx with the key from your portal.
OBSRVBL_SERVICE_KEY="kjjkhakjdsjhj2342kjhadsk"
```

Figure 20. Service key in the config.local file.



The screenshot shows a terminal window titled "swcadmin@centos:~". The window title bar also displays "GNU nano 2.3.1", "File: /opt/obsvb1-ona/config.local", and "Modified". The main content of the terminal shows the configuration file "config.local" with the following content:

```
OBSRVBL_ONA_NAME=Dcloud_SWC_Sensor
OBSRVBL_NETWORKS="10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 198.19.10.0/24 198.19.20.0/24"
OBSRVBL_IPFIX_CAPTURER="true"
OBSRVBL_IPFIX_PROBE_34_PORT="2055"
OBSRVBL_IPFIX_PROBE_34_PROTOCOL="udp"
OBSRVBL_IPFIX_PROBE_34_TYPE="netflow-v9"

OBSRVBL_ETA_CAPTURER="true"
OBSRVBL_ETA_PCAP_DIR="/opt/obsvb1-ona/logs/eta"
OBSRVBL_ETA_CAPTURE_IFACE="any"
OBSRVBL_ETA_CAPTURE_SECONDS="600"
OBSRVBL_ETA_CAPTURE_MBITS="32"

OBSRVBL_ISE_POLLER="true"
OBSRVBL_ISE_SERVER_NAME="admin.dcloud.cisco.com"
OBSRVBL_ISE_CLIENT_CERT="/opt/obsvb1-ona/certs/swc-sensor_198.19.20.143.cer"
OBSRVBL_ISE_CLIENT_KEY="/opt/obsvb1-ona/certs/swc-sensor-decrypted.key"
OBSRVBL_ISE_CA_CERT="/opt/obsvb1-ona/certs/CertificateServicesRootCA-admin_.cer"

OBSRVBL_SERVICE_KEY="kjjkhakjdsjhj2342kjhadsk"
```

At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts for navigating the nano editor.

Once the key has been added and the service started on the sensor, it will begin a heartbeat process to announce and start a sync with the cloud portal. **This process usually takes about 15 minutes to fully complete.** When finished the sensor icon will be green and the name of the sensor will appear in the sensor list. We will continue working in the lab while this happens in the background.

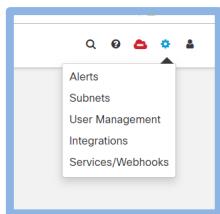
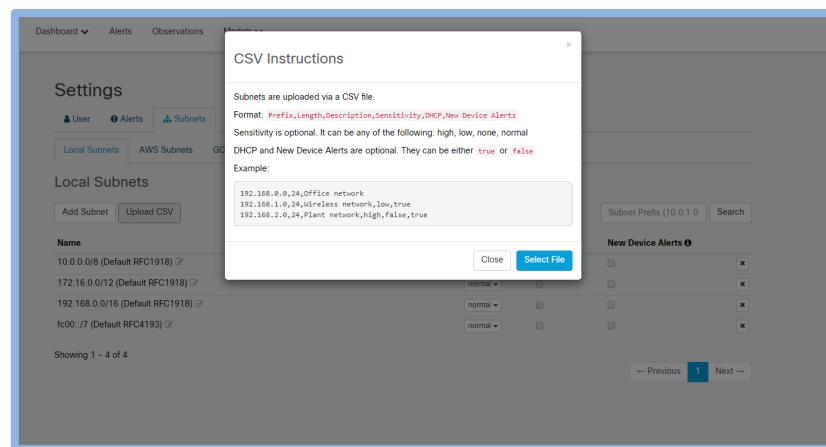
Initial Stealthwatch Cloud Portal Configuration

As part of most new software installs there are typically recommended settings, in this section you will configure your new portal for some initial settings. We will start with configuring the subnet used in the lab and then creating a watchlist. By default Stealthwatch Cloud monitors any of the RFC 1918 private space and has them all set at “normal” sensitivity. In this lab we use both private and public IP spaces, so we need to add those public subnets so the Stealthwatch Cloud service will consider them internal, additionally we will label our subnets for easier reference, users can also select the sensitivity of the subnet. This sensitivity instructs our modeling engine to apply more scrutiny to subnets that are considered higher value vs ones that change frequently (e.g, guest wireless) or have limited importance.

[Configure public subnet used in Dcloud in your SWC portal.](#)

Since this is a new portal, we need to tell it what subnets are being used in Dcloud.

1. Login to the Stealthwatch Cloud portal
2. Select the settings icon on the upper right corner then Subnets, see figure 21.
3. Select Upload CSV, use the subnet.csv file that was downloaded using GitBash.
(downloads/lab-swc/subnets.csv)

Figure 21. Subnet location**Figure 22.** Subnet CSV Upload

Note: You may receive the following error. Ignore as it's benign:

Local Subnets

AWS Subnets GCP Subnets VPN Subnets Azure Subnets

Local Subnets

(!, <HTTPStatus.CREATED: 201>)

Add Subnet Upload CSV

- Once uploaded the subnet labels will match what is configured in Dcloud

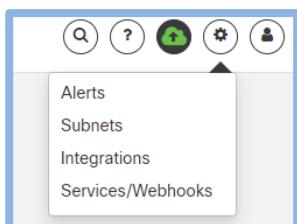
Figure 23. Local Subnets

Name	Sensitivity	Static	New Device Alerts
10.0.0.0/8 (Default RFC1918) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
10.201.0.0/24 (Data Center 01) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
10.201.3.0/24 (User Subnet) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
172.16.0.0/12 (Default RFC1918) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
172.16.16.0/24 (Core Network) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
192.168.0.0/16 (Default RFC1918) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
198.18.1.0/24 (Remote VPN) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
198.19.10.0/24 (DataCenter 02) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
198.19.20.0/24 (DataCenter 02) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
198.19.30.0/24 (DataCenter 02) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
209.182.184.0/24 (Data Center 01) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X
fc00::/7 (Default RFC4193) <i>✓</i>	normal ▾	<input type="checkbox"/>	<input type="checkbox"/> X

Configure a TOR Watchlist in the Stealthwatch Cloud portal

In this company using the TOR network is prohibited. We are going to configure the Stealthwatch Cloud portal to pull TOR exit nodes from a 3rd party website allowing us to see if users are using that service. The watchlist URL is located in the wkst1_command.text file for easy copy/paste into the portal

- Login into the Stealthwatch Cloud portal
- Select **Alerts** in the upper right-hand window

Figure 24. Alerts Menu

3. Select **Configure Watchlists**
4. Select **Third Party Watchlists**
5. Enter a description in the name field.

Note – The link below is located in the wkst1_commands.txt file located in /downloads/lab-swc

- a. Resource = https://onstatic.s3.amazonaws.com/oneoff/combined_tor.txt
- b. Check Never Expire
- c. Check Bidirectional Traffic
- d. Select Add

Figure 25. Third Party Watchlist

Name	Watchlist URL	Threshold	Bidirectional	Reason	Status
This list is empty.					

Add Resource

Name: Devices using Tor

Resource*: https://www.dan.me.uk/torlist/

Never Expire

Expiration Date*: 1

Threshold*: 1

Bidirectional traffic only

Reason: Reason for this entry

+ add

Sensor NetFlow Collection

The sensor you added previously should now be available in the portal. You will need to configure the flow settings that we imported to the UDP Director.

1. Select cloud icon in the upper left, then sensors.

Figure 26. Sensors Icon



2. Select the **Change Settings** button on the Dcloud sensor, then select the **NetFlow/IPFIX** tab, configure the settings as show in figure 28.

Figure 27. Active Sensors

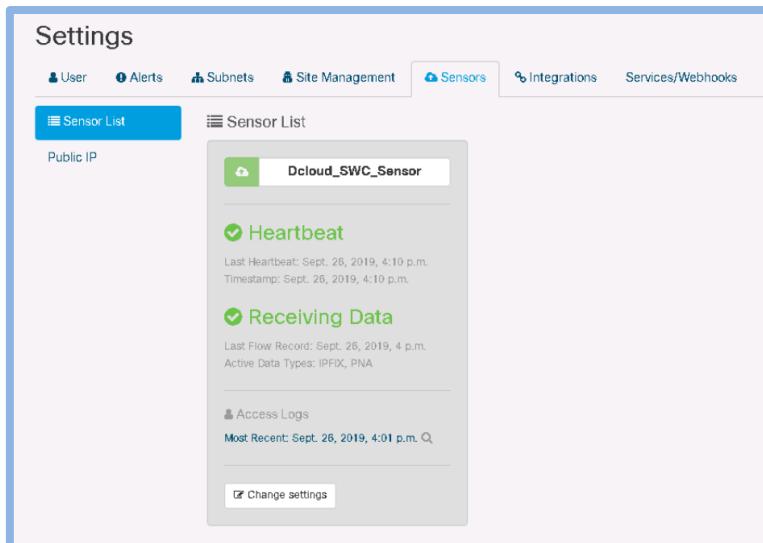
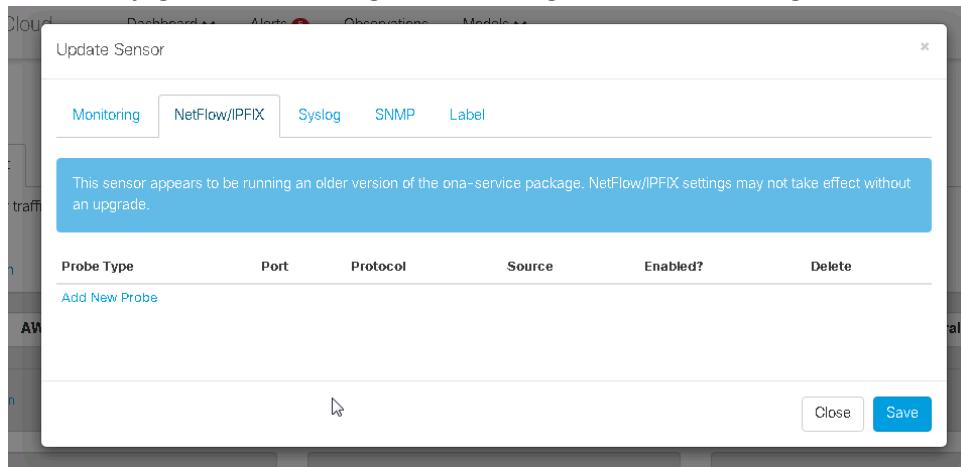


Figure 28. Flow Configuration Settings

Update Sensor

Monitoring	NetFlow/IPFIX	Syslog	SNMP	Label	
Probe Type	Port	Protocol	Source	Enabled?	Delete
NetFlow v9	9995	UDP	Standard	<input checked="" type="checkbox"/>	Delete
IPFIX	4739	UDP	Standard	<input checked="" type="checkbox"/>	Delete
NetFlow v9	9997	UDP	Cisco ASA Device	<input checked="" type="checkbox"/>	Delete
Add New Probe					
Close Save					

Note: You may get the following sensor image version message. Please ignore:



3. Next set the sensor label to a personalized name, do this by selecting **Label** and entering a name. Select **Save** to save both changes. The sensor periodically checks the portal for updates, when a new configuration is detected it updates /opt/obsrvbl-ona/config.auto.

Update Sensor

Monitoring	NetFlow/IPFIX	Syslog	SNMP	Label
Label: <input type="text" value="Cisco Fan!"/>				
Close Save				

At this point the sensor is collecting data and sending to the Stealthwatch Cloud back-office ~every 15 minutes. You can see the last time a heartbeat and data were collected by clicking on the Green cloud icon.

The active data types show what the sensor is collecting, the default configuration of the sensor is to create flow data from any traffic on any of its network interfaces. This is mainly used for networks that are feeding the sensor with SPAN. However, it will also generate flows for the traffic hitting the management interface even if SPAN is not used, flows created from interface traffic show up as “PNA”. If a sensor is configured and able to receive flow traffic such as IPFIX or NetFlow then the “IPFIX” data type will also be displayed. In this lab we would expect to see both. Initially it will display PNA, once the NetFlow configuration is pushed down and files are uploaded IPFIX will be displayed.

Figure 29. Sensor Status

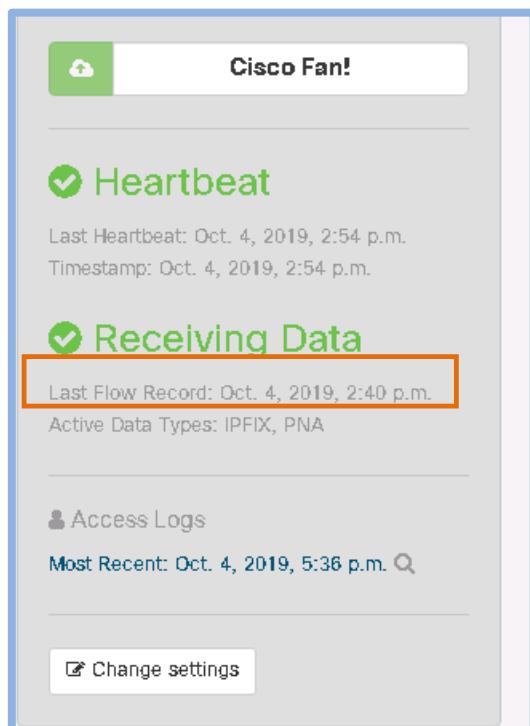
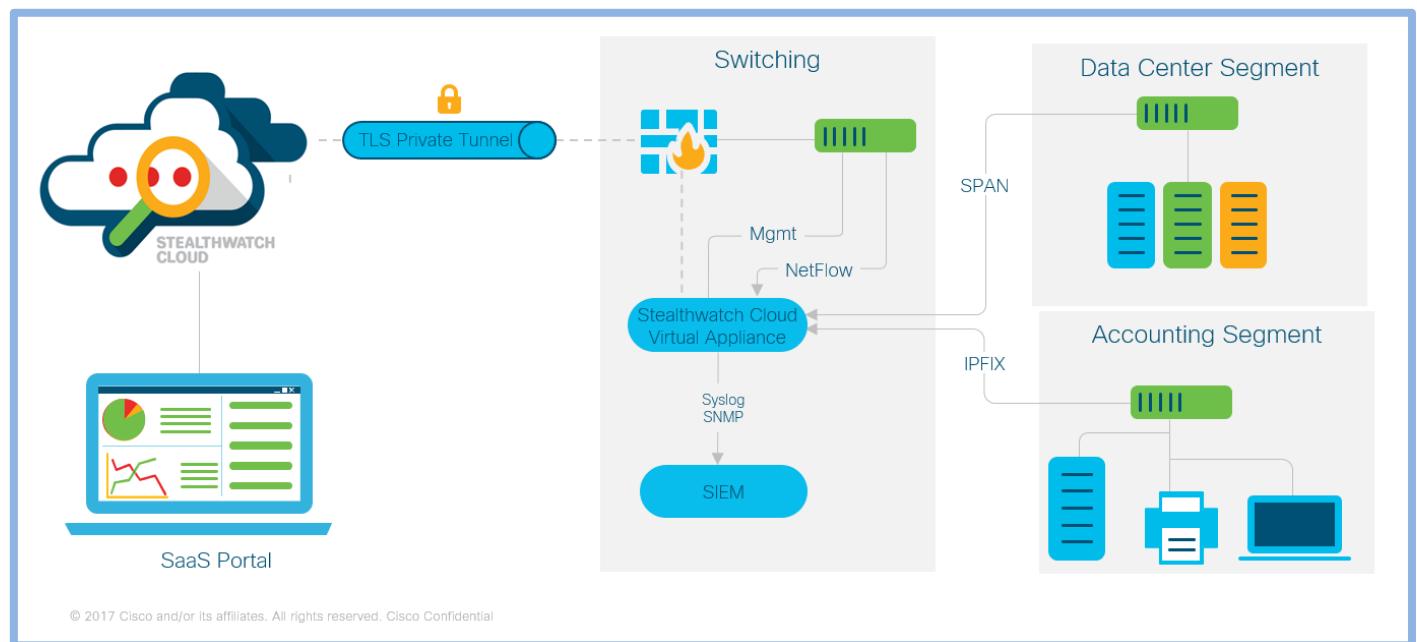


Figure 30. Sensor Network Deployment Capabilities and Options



Workstation Setup

Validating Your Workstation 1 – Install Tor Browser

In this lab, you will install the Tor browser to generate traffic and validate results. All network traffic generated by the Workstation 1 will be accounted for by NetFlow records, stored as a network audit trail and used to detect threats east and west inside the network and north and south to the Internet. Refer to screenshot shown below.

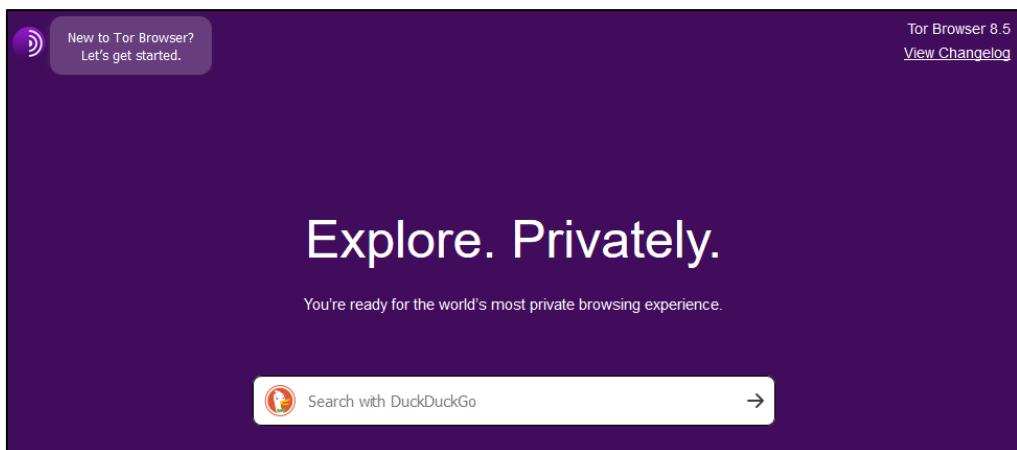
1. Open **Chrome** from the desktop of the Workstation 1 and select the Tor Project Link in the browser or go to <https://www.torproject.org/download>
2. Click the Windows Sign to **Download the Tor** installation file.
3. Install **torbrowser .exe** using all default settings. Make note of the file size of the .exe download which is ~52 MB; you will search for this in an upcoming lab.

Figure 31. Install Tor Browser



4. Click **Start Tor Browser** from the desktop, click Connect when Tor launches and search for “**what is flexible NetFlow**”, shown below.
 - a. Skim through a few articles and perform other searches to generate traffic through the Tor network. Make note that everything being searched is encrypted through the browser.
 - b. Keep the **Tor Browser** open for the next exercise.

Figure 32. Search within the Tor Browser



Validating Your Workstation 1 – netstat

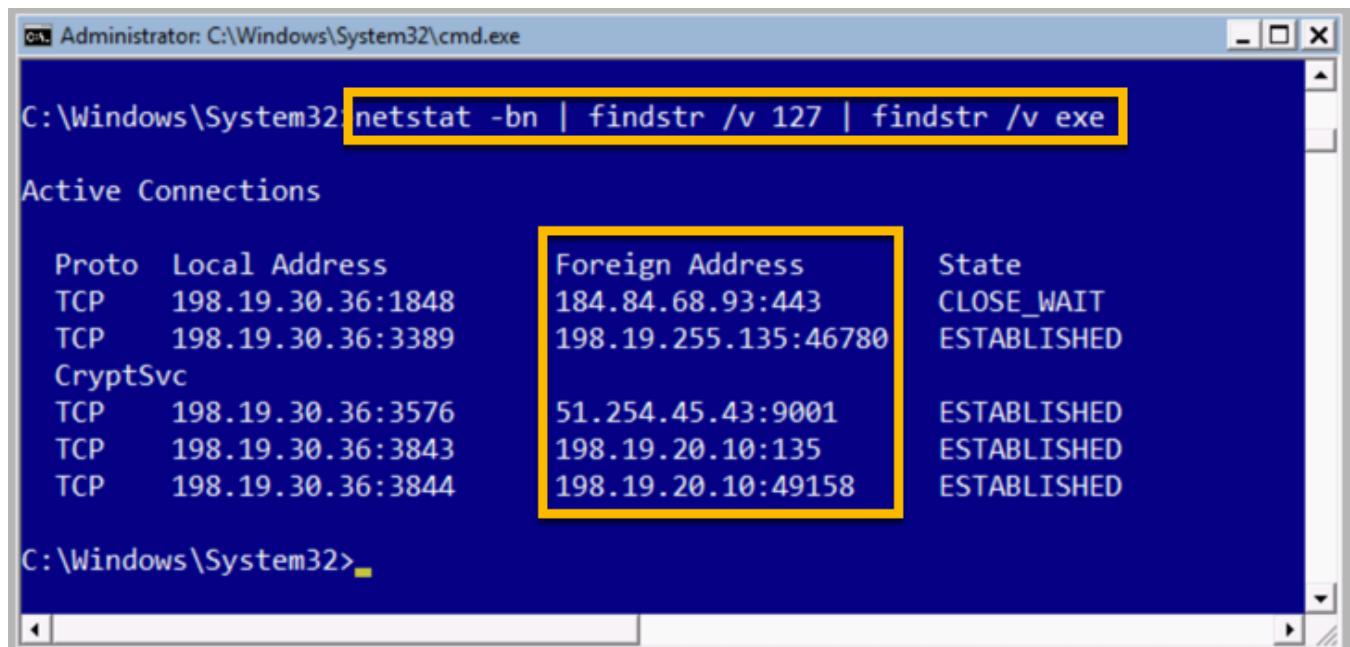
This lab will use the netstat (network statistics) command line tool to display incoming and outgoing network connections from Wkst1. It will also show that those connections will be accounted for through NetFlow. You are using netstat to see what connections exist to validate being able to search Stealthwatch for any active or historical network conversations.

The Wkst1 commands are also located in the Wkst1_commands.txt file in the downloads/lab-swc directory for easier typing. From the **cmd.exe** window, type **netstat -bn | findstr /v 127 | findstr /v exe**

The ‘-n’ is needed to not perform name resolution so you can see the Foreign IP address being connected to. The ‘-b’ will display process name. The findstr /v command will filter the results to display less information as shown below. Make note of the Foreign IP addresses being connected to. You will be able to search Stealthwatch for historical network conversations to and from the WKST1 IP address.

Note: Leave the command prompt open for later use

Figure 33. netstat utility



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\System32 netstat -bn | findstr /v 127 | findstr /v exe

Active Connections

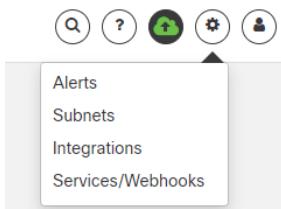
  Proto  Local Address          Foreign Address        State
  TCP    198.19.30.36:1848      184.84.68.93:443    CLOSE_WAIT
  TCP    198.19.30.36:3389      198.19.255.135:46780 ESTABLISHED
CryptSvc
  TCP    198.19.30.36:3576      51.254.45.43:9001  ESTABLISHED
  TCP    198.19.30.36:3843      198.19.20.10:135   ESTABLISHED
  TCP    198.19.30.36:3844      198.19.20.10:49158  ESTABLISHED

C:\Windows\System32>
```

Configure Country Watchlists in the Stealthwatch Cloud portal

As part of the modeling engineer, Stealthwatch Cloud Geo-codes all external IPs to their origin country, this is valuable as it lets you see what countries a machine or network normally communicates with. Stealthwatch Cloud allows users to configure which countries represent “high-risk” for their organization, normally these would be countries that you don’t have offices in or normally do business with, when a country is set as “high-risk” traffic to it is flagged with special observations, in addition if certain actions are detected from one of those countries, such as a remote login, or a long heartbeat, an alert would be generated. In this lab we are going to select the United States, Germany, France, China, and any other you would like. Later, in a future exercise we will review how to see the results of doing this.

1. Login into the Stealthwatch Cloud portal
2. Select **Alerts** in the upper right-hand window

Figure 34. Alerts Menu

3. Select [Configure Country Watchlists](#)
4. Select the United States, Germany, France, China, and any other you would like, then select [Add Selected](#). Note: Some countries may already be selected. Please leave them selected if so.

Figure 35. Country Watchlist Settings

Country Watchlist Settings

Watchlisted Countries

Germany United States

[Remove Selected](#) | [Select All](#)

Available Countries

[Add](#)

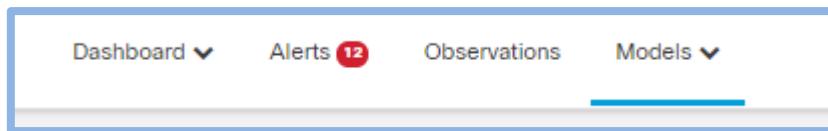
[Add Selected](#) | [Select All](#)

Afghanistan Aland Islands Albania Algeria American Samoa Andorra Angola Anguilla Antarctica
 Antigua and Barbuda Argentina Armenia Aruba Australia Austria Azerbaijan Bahamas Bahrain
 Bangladesh Barbados Belarus Belgium Belize Benin Bermuda Bhutan Bolivia Bosnia and Herzegovina
 Botswana Bouvet Island Brazil British Indian Ocean Territory Brunei Darussalam Bulgaria Burkina Faso Burundi
 Cambodia Cameroon Canada Cape Verde Caribbean Netherlands Cayman Islands Central African Republic Chad
 Chile China Christmas Island Cocos (Keeling) Islands Colombia Comoros Congo Congo Cook Islands

Pause Here for Public Cloud Monitoring Lecture – Approx 30 minutes.

Portal Overview

We will cover the basic menu structure of the portal in this section and then focus on how to flow queries.

Figure 36. Portal Menu's

Dashboard – This contains our standard and network centric dashboard. The network dashboard has additional information on top talkers, traffic to high risk countries, amount of encrypted traffic.

Alerts – A list of all open alerts, additional section criteria available for closed, snoozed, assigned, etc.

Observations – We cover what observations are in more detail later, this menu has various ways of seeing the collected Observations.

Models – This contains various reports and queries.

Endpoints – All endpoints sorted by total connections

Traffic traffic – Summary report of top ports, IPs for a selected time period

Session Traffic – Flow data query

Roles – Types of detected device types (this is a new portal and this will be empty)

Encrypted Traffic – Similar to flow query, allowing you to search by ciphers

External Services – List of common external services that are used in the network (this is a new portal and this will be empty)

Users – Stealthwatch cloud can pull in traffic from ISE or some cloud environments, this page displays user login data

Stealthwatch Cloud – Flow Search

A powerful tool inside Stealthwatch Cloud is the ability to query and visualize the flow data. This section will guide you on how to use this feature and pivot out of it to do additional investigations.

1. Login to your Stealthwatch Cloud portal, via Wkst1.

2. Select **Models > Session Traffic** from the menu bar. Session Traffic is used to query against the database of flows that Stealthwatch Cloud has. For example, you could run a query to see what DNS servers are being used, who is hosting web servers, etc.

Figure 37. Stealthwatch Cloud Flow Query

Session Traffic

active filters

Filter by a list of IPs or CIDR ranges. Use "-" to exclude an IP (e.g. "10.0.0.1, 10.0.1.0/24, -10.0.1.7").

IP	IP, host ...
Connected IP	IP, host, ...

Filter by a list of ports or port ranges. Use "-" to exclude a port. (e.g. "22-25, 80, -443").

Port	port or range of ports
Connected Port	port or range of ports

Filter by low-level protocol.

Protocol	All
-----------------	-----

Filter by bytes or packets.

Bytes to	Min	Max	Bytes from	Min	Max
Packets to	Min	Max	Packets from	Min	Max

Enter a start date/time and end date/time for the search. Longer time ranges will take longer to load.

Start Date	2019-07-25	Start Time	00:00
End Date	2019-07-25	End Time	23:59

Update

The top portion of the Flow Search window will show the filter criteria. In this sample query we are going to look at the communication the sensor has been making.

1. Enter the Stealthwatch Cloud Sensor address of **198.19.20.143** into the IP field.
2. Enter **443** in the Connected Port. **Note:** that we are limiting the flow query to encrypted https or 443/tcp connections.
3. Leave Connected IP empty, this will allow to search for any 443 sessions.
4. Hit **Update** to begin running the flow query of any connection on this day between your sensor and the Internet on 443/tcp, as shown below.

Figure 38. Filter settings

Session Traffic

Q active filters

Filter by a list of IPs or CIDR ranges. Use "-" to exclude an IP (e.g. "10.0.0.1, 10.0.1.0/24, -10.0.1.7").

IP IP, host ...

Connected IP

Filter by a list of ports or port ranges. Use "-" to exclude a port. (e.g. "22-25, 80, -443").

Port

Connected Port port or range of ports

Filter by low-level protocol.

Protocol

Filter by bytes or packets.

Bytes to	<input type="text" value="Min"/>	<input type="text" value="Max"/>	Bytes from	<input type="text" value="Min"/>	<input type="text" value="Max"/>
Packets to	<input type="text" value="Min"/>	<input type="text" value="Max"/>	Packets from	<input type="text" value="Min"/>	<input type="text" value="Max"/>

Enter a start date/time and end date/time for the search. Longer time ranges will take longer to load.

Start Date **Start Time**

End Date **End Time**

Update

1. Click the **black triangle** next to an external IP address to see more context about it or perform additional searches. Select **Talos Intelligence** to see more details on what Talos knows about the external IP address.

Session Traffic									
active filters start time: 2020-01-01T00:00; end time: 2020-01-01T23:59; ip: 198.19.20.143; connected_port: 443;									
Traffic Traffic Chart Connections Graph									
Table of matching sessions.									
20 records per page									
<th>Time</th> <th>IP</th> <th>Connected IP</th> <th>Port</th> <th>Connected Port</th> <th>Protocol</th> <th>Bytes</th> <th>Packets</th>	Time	IP	Connected IP	Port	Connected Port	Protocol	Bytes	Packets	
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
1/1/20 11:58 PM	198.19.20.143	107.22.217.211	53792	443 (https)	0	6,260	0	11	0
1/1/20 11:58 PM	198.19.20.143	107.22.217.211	53792	443 (https)	TCP	7,412	2,095	11	12
1/1/20 11:58 PM	198.19.20.143	107.22.247.3	33960	443 (https)	0	7,977	0	11	0
1/1/20 11:58 PM	198.19.20.143	52.216.109.165	35948	443 (https)	0	4,180	0	16	0
1/1/20 11:58 PM	198.19.20.143	107.22.217.211	53792	443 (https)	TCP	20,660	4,298	26	31
1/1/20 11:58 PM	198.19.20.143	107.22.210.176	57684	443 (https)	0	6,260	0	11	0
1/1/20 11:58 PM	198.19.20.143	107.22.247.3	33960	443 (https)	TCP	9,129	2,090	11	13
1/1/20 11:58 PM	198.19.20.143	107.22.210.176	57684	443 (https)	TCP	7,308	2,051	10	11
1/1/20 11:58 PM	198.19.20.143	52.216.109.165	35948	443 (https)	TCP	5,602	3,777	15	15

Figure 39. Talos Threat Intel Pivot

LOCATION DATA		REPUTATION DETAILS											
No location data available.		? EMAIL REPUTATION ● Neutral ? WEB REPUTATION ● Neutral ? WEB CATEGORY -											
OWNER DETAILS		LAST DAY LAST MONTH											
IP ADDRESS	38.229.72.19	SPAM LEVEL	None None										
?	FWD/REV DNS MATCH	EMAIL VOLUME	0.0 0.0										
?	HOSTNAME	VOLUME CHANGE	0% 0%										
?	DOMAIN	Think this information is incorrect? Submit a Web Reputation or a Web Categorization dispute.											
?	NETWORK OWNER												
BLACKLISTS ? <ul style="list-style-type: none"> BL.SPAMCOP.NET Not Listed CBL.ABUSEAT.ORG Not Listed PBL.SPAMHAUS.ORG Not Listed SBL.SPAMHAUS.ORG Not Listed <p>TALOS SECURITY INTELLIGENCE BLACKLIST</p> <table border="1"> <tr> <td>BLACKLISTED</td> <td>Yes</td> </tr> <tr> <td>CLASSIFICATION</td> <td>Malware</td> </tr> <tr> <td>FIRST SEEN</td> <td>2019-07-04T00:26:46 UTC</td> </tr> <tr> <td>EXPIRATION DATE</td> <td>2019-08-03T00:26:48 UTC</td> </tr> <tr> <td>STATUS</td> <td>ACTIVE</td> </tr> </table>				BLACKLISTED	Yes	CLASSIFICATION	Malware	FIRST SEEN	2019-07-04T00:26:46 UTC	EXPIRATION DATE	2019-08-03T00:26:48 UTC	STATUS	ACTIVE
BLACKLISTED	Yes												
CLASSIFICATION	Malware												
FIRST SEEN	2019-07-04T00:26:46 UTC												
EXPIRATION DATE	2019-08-03T00:26:48 UTC												
STATUS	ACTIVE												

- Add an external IP address to a watchlist by clicking the down arrow and selecting add to watchlist list, name the watchlist whatever you would like.

Figure 40. Custom watchlist pivot

The screenshot shows a table of network traffic logs. The columns include Date, Source IP, Destination IP, Port, and Protocol. A context menu is open over the fourth row, listing options like IP Traffic, Session Traffic, AbuseIPDB, Google Search, Talos Intelligence, Add IP to watchlist (which is highlighted in orange), Find IP on multiple days, and Copy (with the value 13.226.101.92).

10/4/19 2:48 PM	198.19.30.36	174.129.109.99	12594	443 (http)
10/4/19 2:46 PM	198.19.30.36	13.226.101.92	12568	443 (http)
10/4/19 2:45 PM	198.19.30.36			443 (http)
10/4/19 2:45 PM	198.19.30.36			443 (http)
	<input type="button" value="CSV"/>	Showing 1 to 20 of 77		
Conditions statement	What's New FAQ			

Figure 41. Custom IP watchlist

This form allows users to add a new entry to a watchlist. It includes fields for Name, Domain / IP, Bidirectional (checkbox), Reason, Resource, Never Expire (checkbox), Expiration Date (calendar icon), Bidirectional traffic only (checkbox), and a Reason text area. A '+ add' button is at the bottom.

Traffic with the following domains and IPs generates alerts.

Name	Domain / IP	Bidirectional	Reason
This list is empty.			

Add Domain or IP

Name

Resource*

Never Expire

Expiration Date*

Bidirectional traffic only

Reason

Finding Flows using Session Filter

1. Go back to **Models > Session Traffic** from the menu bar.
2. Previously we just searched for 443 traffic. What if we wanted to search all flows except 443? In the session filter you can put a minus sign before the port or IPs to remove data from the flow report.

Enter the sensor IP address of **198.19.20.143** into the IP field. In connected IP enter **-198.19.20.0/24**. In connected port enter **-443**. **This query will show all flows that are from the Stealthwatch Cloud sensor to the 198.19.20.0/24 network and that are NOT 443. Select Update to run the new query and verify the results.

The screenshot shows the 'Session Traffic' search interface. The filters applied are:

- IP:** 198.19.20.143
- Connected IP:** 198.19.20.0/24
- Port:** port or range of ports
- Connected Port:** -443

The search parameters are set to:

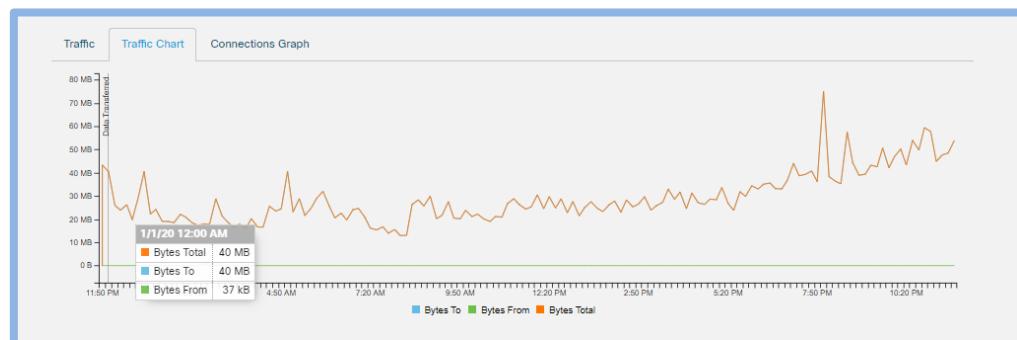
- Start Date:** 2020-01-01
- End Date:** 2020-01-01
- Start Time:** 00:00
- End Time:** 23:59

The results table displays the following data:

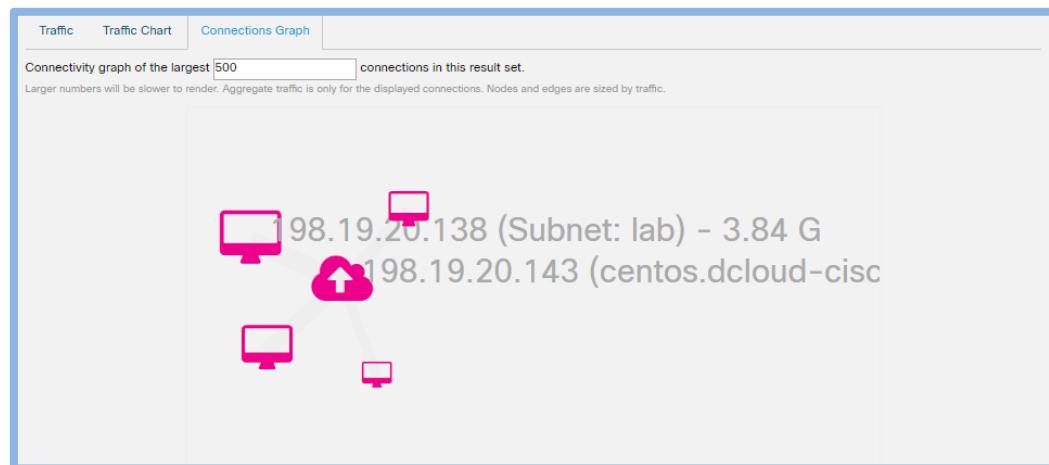
Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	To	From
1/1/20 11:58 PM	198.19.20.143	198.19.20.10	41833	53 (domain)	UDP	370	240	2	2
1/1/20 11:58 PM	198.19.20.143	198.19.20.10	39488	53 (domain)	UDP	366	228	2	2
1/1/20 11:58 PM	198.19.20.143	198.19.20.10	36810	53 (domain)	UDP	370	240	2	2
1/1/20 11:58 PM	198.19.20.143	198.19.20.10	55033	53 (domain)	UDP	370	240	2	2

Figure 42. Custom Flow Query

3. Next, select **Traffic Chart**. This will graph the flow traffic so you can easily understand the volume and if needed narrow the query. It can be difficult to analyze many lines of flows to find the interesting behavior, traffic chart and connections graph a good way to visually see the data.

Figure 43. Flow Query Traffic Chart

4. Next, select **Connections Graph**. This will show the machine connectivity for the flow query . The larger the icon the more traffic was sent to/from it. Click on an icon to see IP address and traffic amounts. You can zoom in using your mouse.

Figure 44. Connections Graph

Finding Flows for the TOR download

1. By now the TOR download should have uploaded to the portal. Start a new session traffic search, in the **Bytes to Min** field, type **50000000** to filter the results to only display flows that were greater than 50 MB of data exchanged, shown below
2. Scrolling through the flows you should see a flow between your Workstation 1, **198.19.30.36**, as the subject connected to an Internet facing peer.
1. In the search below, the ~59 MB download was with **38.229.72.19** out of the US over https. **Note:** The peer IP address may be different from when you downloaded your Tor executable.
2. Notice the **MB size** coming down from the peer to your Workstation 1.
3. Click the **black triangle** next to the external IP address to see more context about it or perform additional searches.

Figure 45. Flow Table Quick view

Time	IP	Connected IP	Port	Connected Port	Protocol	To	From	Bytes	Packets
7/25/19 5:30 PM	198.19.30.36	38.229.72.19	34410	443 (https)	TCP	59,392,299	799,148	43,541	19,885
7/25/19 5:24 PM	198.19.30.36	172.217.15.112	34281	443 (https)	TCP	178,830,597	1,253,952	129,742	31,199

Filter the flow table by one of the Foreign IP addresses with :443 you saw in the netstat lab.

1. Remove the 50000000 value we added earlier in [Bytes to](#)
2. In the **Connected IP field** enter an IP address you observed in your netstat lab above. The IP address may vary from what is listed in the figure below.

Peer IP Address Filter

Figure 46. Session Traffic

Session Traffic

active filters start time: 2019-07-25T00:00; end time: 2019-07-25T23:59; ip: 198.19.30.36; connected_ip: 198.19.20.136; connected_port: 443;

Filter by a list of IPs or CIDR ranges. Use "-" to exclude an IP (e.g. "10.0.0.1, 10.0.1.0/24, -10.0.1.7").

IP	<input type="text" value="198.19.30.36"/> X	IP, host ...
-----------	---	--------------

Filter by a list of ports or port ranges. Use "-" to exclude a port. (e.g. "22-25, 80, -443").

Port	<input type="text" value="port or range of ports"/>
Connected Port	<input type="text" value="443"/> X port or range of ports

Filter by low-level protocol.

Protocol	<input type="text" value="All"/>
-----------------	----------------------------------

Filter by bytes or packets.

Bytes to	<input type="text" value="Min"/>	<input type="text" value="Max"/>	Bytes from	<input type="text" value="Min"/>	<input type="text" value="Max"/>
Packets to	<input type="text" value="Min"/>	<input type="text" value="Max"/>	Packets from	<input type="text" value="Min"/>	<input type="text" value="Max"/>

Enter a start date/time and end date/time for the search. Longer time ranges will take longer to load.

Start Date	<input type="text" value="2019-07-25"/>	Start Time	<input type="text" value="00:00"/>
End Date	<input type="text" value="2019-07-25"/>	End Time	<input type="text" value="23:59"/>

[Update](#)

Summary

In this Getting Started lab, you:

- Became familiar with your Workstation that you connected to in the data center
- Learned that all network conversations are accounted for from this machine through NetFlow collection
- Learned how to run a basic Flow Search in Stealthwatch Cloud to see all https flow between your Workstation and the Internet.
- Understood some basic Stealthwatch Cloud configuration features

End of Lab: Please pause here.

Breach Detection

To help get in the mind of an attacker, take a minute to read through the persona of “Harry the Hacktivist” and how he operates. Understanding the attacker can help build solutions to defend your organization.



“I use the internet as a political megaphone. Fight the power! ”

Goals

- ① Public disruption of service of the target
- ② Defacing Social Media Accounts of Criminal Organizations
- ③ Exposing injustices and hypocrisies of governments

Attack Vectors

DDoS Network Infiltration Social Engineering
Doxing Website Defacement

Age: 12-60
Location: Global
Description: Hacktivists are not motivated by profit. They hack to promote their political or societal agenda. Hacktivists will go after enemies that are perceived to be in their way, including those that they believe are unjust.

Mitigation Techniques

- DDoS scrubbing
- Host lock devices and appliances being used for data exfiltration
- Employee education in security procedures to prevent exposure of sensitive data via social engineering

Expertise

Security: NOVICE EXPERT
Networking: NOVICE EXPERT

SecOps Strategy

 GUARD Guard against DDoS and related events. Manage evolving impacts associated with events.	 SPIKES Track spikes on new or unusual connections to external hosts	 MONITOR Monitor for web-based attacks such as SQL injection
---	--	--

Lab 1: Remote Access Breach using stolen credentials

Business Objectives

According to the Ponemon Institute 2017 Cost of Data Breach Study of 419 companies in 13 countries, \$3.62 million is the average total cost of a data breach. To help combat this, it is critical to try to account for 100% of network conversations to detect threats that bypass traditional monitoring solutions.

Test Drive Objectives

In this test drive, you will see first-hand the importance of capturing flow data from as close to the endpoints as possible to be able to account for all active and historical network conversations.

Test Drive Requirements

- Stealthwatch Cloud Portal

Test Drive Outline

- Task 1. Connect to a server running Remote Desktop within a datacenter
- Task 2. Download an exploit-kit
- Task 3. Perform network scanning reconnaissance
- Task 4. Install exploit-kit
- Task 5. Investigate Security Events generated in Stealthwatch Cloud

Task 1: Connect to a Remote Desktop server within a data center

Below is a list of realities of why you need to build stronger defenses beyond access control lists or firewalls:

- Firewalls are as good as the person implementing them, mistakes happen.
- If the access control policy is misconfigured and an any-any rule is moved to the top, how would you detect this before it's too late?
- Detect threats when an authorized server is used with stolen credentials.
- Account for all traffic on the inside of the firewall so you can build a general ledger of both authorized and non-authorized traffic making it through the firewall and provide a second chance detection.

Scenario: You have been performing reconnaissance against an organization and have identified a remote desktop server that is exposed to the Internet. You have discovered the below credentials to the server and begin building a foothold inside the organization. In this lab, you will need to access Workstation 1, which gives you access to all data center resources.

Note: If Remote Desktop is already up, move to Task 2.

Click **Remote Desktop** link to launch a web Remote Desktop session built within dCloud shown below.

Note: Username: wkst\Administrator Password: C1sco12345

Figure 47. Workstation1 Remote Desktop

You are now inside the organizations data center by leveraging a server exposed to the Internet and using stolen credentials!

Task 2: Download an exploit-kit (this was already done previously)

The exploit Kit is located in the downloads/lab-swc directory

Task 3: Perform network scanning reconnaissance

One of the first phases of any attack is reconnaissance. Various open source tools are available to attackers. In order to break the Cyber Kill Chain, tools must be able to identify when this type of attack is occurring.

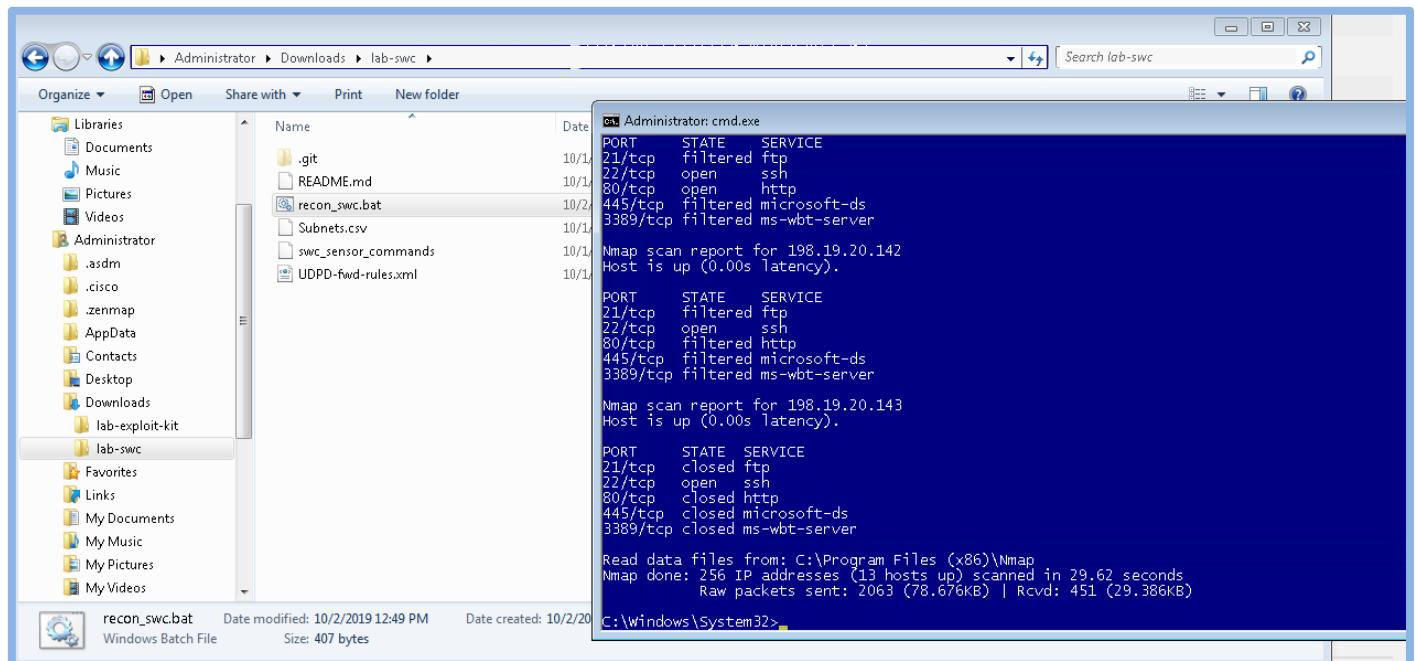
In Task 3, we will assume the attacker is already in the network, selecting targets through scanning activity, and attempting to identify vulnerabilities in the target network.

Perform these steps to initiate an attack against the target network to identify additional resources in the data center.

From the Remote Desktop session of WKST1 in the dCloud lab:

1. Open the **lab-swc** folder that was downloaded from GitHub within the Downloads directory.
2. We are searching for common management ports such as 22 = ssh, 23 = telnet, and 3389 = Remote Desktop, etc.. Run the **recon_swc.bat** as illustrated below to perform reconnaissance and find other devices within the network.
3. The recon.bat will pause so you can see the below nmap scan is what is running. Press any key to continue the scan.

```
nmap -n -v -p 21,22,23,25,80,443,3389 10.201.0.0/24 198.19.20.0/24 --disable-arp-ping
```

Figure 48. nmap scan

Note: The scan could take over 5 minutes to complete. When complete, you will see results similar to those shown in the screenshot below.

Make note of the number of hosts scanned and scroll through to see what hosts are listening on given ports.

What does this command mean?

-n: Tells Nmap to *never* do reverse DNS resolution on the active IP addresses it finds. Since DNS can be slow even with Nmap's built-in parallel stub resolver, this option can slash scanning times.

-v: verbose meaning show the contents on the screen.

-p: Port scan on multiple ports. In this case ports 22, 23 and 3389

--disable-arp-ping: Nmap normally does ARP or IPv6 Neighbor Discovery (ND) discovery of locally connected ethernet hosts, even if other host discovery options such as -Pn or -PE are used. To disable this implicit behavior, use the --disable-arp-ping option.

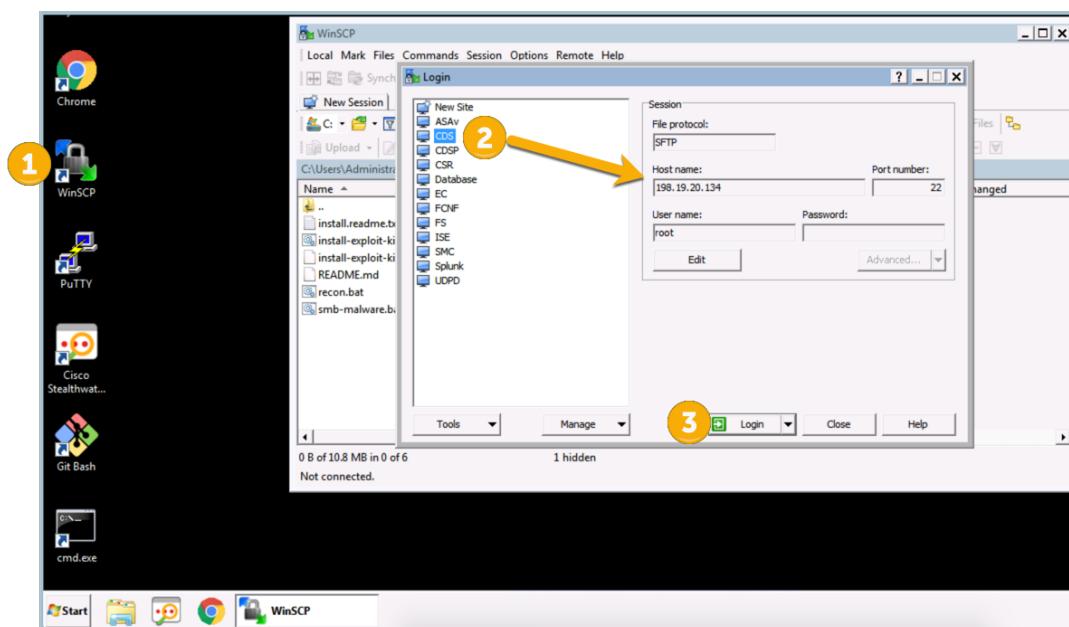
The default behavior is normally faster, but this option is useful on networks using proxy ARP, in which a router speculatively replies to all ARP requests, making every target appear to be up according to ARP scan.

Task 4: Install exploit-kit

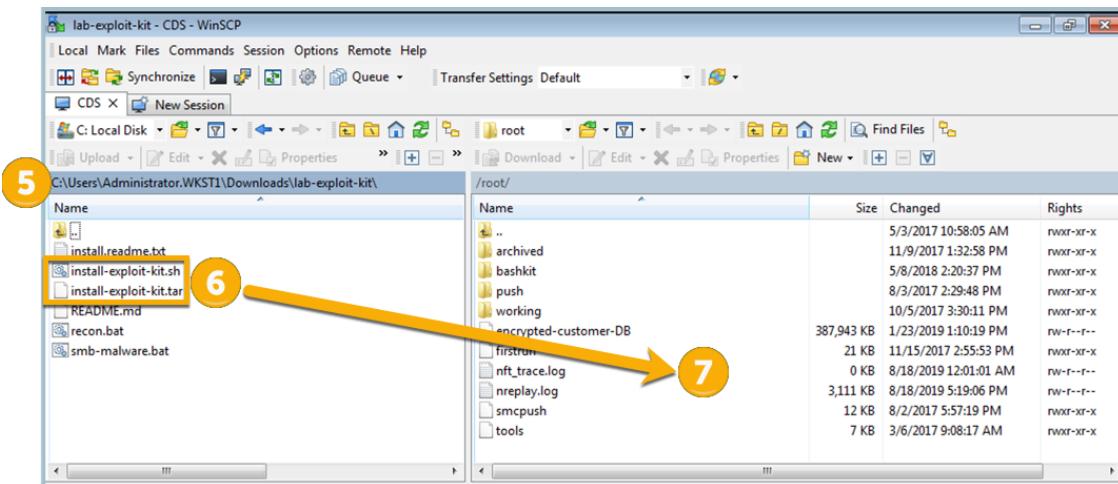
Let's SCP and install the exploit-kit on one of the servers identified during the network scan.

1. Open **WinSCP** from the Desktop as shown below. **Note:** If an update appears, ignore the update.
2. Select **CDS**, as shown below.
3. Select **Login**, the password is pre-saved.

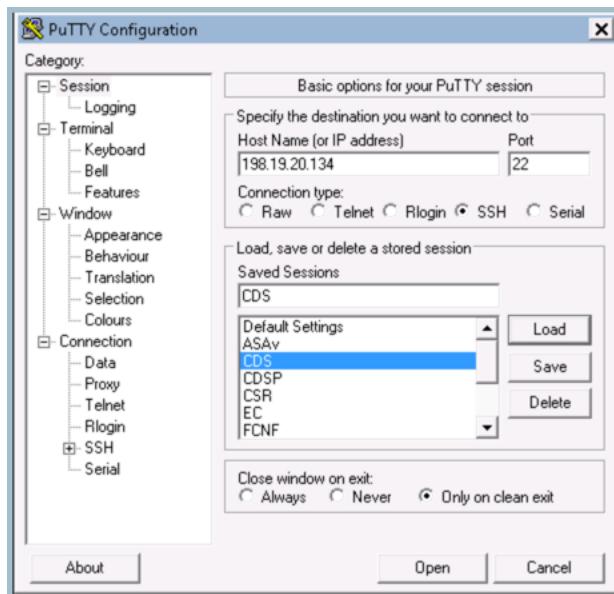
Figure 49. Login WinSCP



5. Within the left panel of **WinSCP**, browse to c:\Users\Administrator.WKST1\Downloads\lab-swc\lab-exploit-kit on the left-hand navigation pane, as shown below.
6. **Highlight** `install-exploit-kit.sh` and `install-exploit-kit.tar`
7. **Drag and drop** `install-exploit-kit.sh` and `install-exploit-kit.tar` within **root** in the right pane, as shown below.
8. Close WinSCP when the transfer is complete.

Figure 50. WinSCP

9. Open Putty located on the Wkst1 desktop and use the **CDS** session to **SSH** into **198.19.20.134** (which is the server we installed the exploit-kit on) with username of **root**.
10. Enter the password **C1sco12345** when prompted in the Putty session window.

Figure 51. Putty

11. Once logged in, enter **pwd** (preset working directory) to make sure you are in the **root** directory. This is where you placed the exploit files.

12. Run the following command `./install-exploit-kit` as shown below to install the tools used to create a foothold within the organization. This command is also listed in the `wkst1_command.text` file used previously. Ignore the errors, we bought this exploit kit on Amazon and it only had a 3 star rating.
13. Run `ls -l` and make note that the exploit kit has captured a customer database with the name `encrypted-customer-DB`. You can exit out of the SSH session.

Figure 52. WinSCP

The screenshot shows a WinSCP terminal window titled 'CDS'. The terminal output is as follows:

```

[root][CDS][~]# pwd
/root
[root][CDS][~]# ./install-exploit-kit
Install complete.

[root][CDS][~]# ls -l
total 402148
drwxr-xr-x 2 root root    4096 Nov  9  2017 archived
drwxr-xr-x 4 root root    4096 May  8  2017 bashkit
-rw-r--r-- 1 root root 397253194 Sep  7 14:49 encrypted-customer-DB
-rw-r--r-- 1 root root   21175 Nov 15  2017 firstrun
-rw-r--r-- 1 root root    4089 Sep  7 14:46 install-exploit-kit
-rw-r--r-- 1 root root    4179 Sep  7 14:48 install-exploit-kit.sh
-rw-r--r-- 1 root root 11325952 Sep  7 14:48 install-exploit-kit.tar
-rw-r--r-- 1 root root      0 Sep  7 00:01 nft_trace.log
-rw-r--r-- 1 root root 2724848 Sep  7 14:49 nreplay.log
drwxr-xr-x 3 root root    4096 Aug  3  2017 push
-rw-r--r-- 1 root root 11949 Aug  2  2017 smcpush
-rw-r--r-- 1 root root   6926 Mar  6  2017 tools
drwxr-xr-x 4 root root    4096 Oct  5  2017 working
[root][CDS][~]#

```

Annotations with yellow circles and arrows:

- Circle 11: Points to the command `pwd` and its output `/root`.
- Circle 12: Points to the command `./install-exploit-kit` and its output `Install complete.`
- Circle 13: Points to the command `ls -l` and its output, specifically highlighting the file `encrypted-customer-DB`.

Task 5: Investigate Security Events Generated in Stealthwatch Cloud

Stealthwatch Cloud will have stored flow records for all north-south connections and east-west connections to the Remote Desktop server and detected the attack traffic that was initiated in the previous lab.

1. Login to the Stealthwatch Console if not already logged in. There can be up to a 30 minute delay between when events happen in the network and when they appear in the

Stealthwatch Cloud portal, while the recent flow data is processed, we are going to review some other features of Stealthwatch Cloud

2. Observations are the building blocks for alerts in Stealthwatch Cloud, they can be thought of simply as facts about the network devices or users that can be classified. As traffic is observed and patterns are detected they are tracked as an observation, over time these being to tell us about the behavior of a user or machine. Stealthwatch Cloud has approximately 75 Observation types ranging from ones focused on public clouds like AWS & Azure or more generic ones that identify network heartbeats, watchlist interactions, traffic outliers, and more. An Observation should not be considered an alert, rather they feed into our entity modeling engine to produce alerts for known bad behavior (e.g. scanning) or to detect behavior deviations that indicate something should be investigated.

Go to the Observations tab in the Stealthwatch Cloud portal, you will see three tabs below it, **Recent Highlights**, **Types**, and **By Device**. Click on **Types** to see the various Observations that Stealthwatch can detect. They are listed in Alphabetical order, you will notice many are not limited to network traffic.

Figure 53. Observation List

Observation Type	Count	Description
Additional Observation	(0)	Additional information about this source.
Amazon GuardDuty API Call Finding	(0)	Amazon GuardDuty reported a suspicious API call.
Amazon GuardDuty DNS Request Finding	(1)	Amazon GuardDuty reported a suspicious DNS request.
Amazon GuardDuty Network Connection Finding	(2)	Amazon GuardDuty reported a suspicious network connection.
Amazon Inspector Finding	(25,176)	A finding was reported for an AWS resource.
Anomalous Profile Observation	(1)	Device(s) used a profile for the first time which differs from typical behaviors seen in the network (e.g., an abnormally high number of devices using the profile for the first time, sending anomalous traffic)
AWS API Watchlist Access Observation	(0)	AWS API was accessed from an IP on a watchlist

Selecting **By Device**, will sort all the network endpoints by Observation count. This can be useful to see what hosts might need to be looked at in more detail. Since our portal is new this is most likely blank but will begin to fill in. Below is an example of what a normal view would look like.

Figure 54. Observations By Device

Observations		
	Count	Last Observation Time
Recent Highlights	10	10/4/19 8:00 AM
Types	148,396	10/4/19 8:09 AM
By Device	144,700	10/4/19 8:26 AM
Device	138,876	10/4/19 9:54 AM
10.0.5.254	119,475	10/4/19 9:54 AM
10.0.7.5	101,055	10/4/19 8:20 AM
10.0.6.43	95,379	10/4/19 8:40 AM
Network	51,649	10/4/19 8:58 AM
site-production-elb	41,236	10/4/19 5:41 AM
obsrvbl-sensor-2019081615240548070000001-asg	32,950	10/1/19 12:00 AM
site-staging-elb	28,055	10/3/19 12:00 AM
i-069939c19e2b01329		
obsrvbl-production-onworker-rq_default-2019090517...		
obsrvbl-production-onworker-rq_default-2019091218...		
CSV	Showing 1 to 10 of 4,009	
	First	Previous
	1	2 3 4 5 6 ... 401

3. Go the settings icon, then Alerts, then select [Configure Alert Priority](#) to see the various types of alerts that are included with the service. Notice how each have a historical data requirement, the longest baseline for Stealthwatch Cloud is 36. The majority of the alerts built-in and will auto enable after hitting their baseline period, others such as the User Watchlist Alert would only generate if a user configured a watchlist such as we did earlier with the TOR network.

Figure 55. Alerts Menu

The screenshot shows a list of alert types and their descriptions. Each alert entry includes a priority level (e.g., Normal priority, Low priority) and a history requirement (e.g., 36 days, 0 days). The alerts listed are:

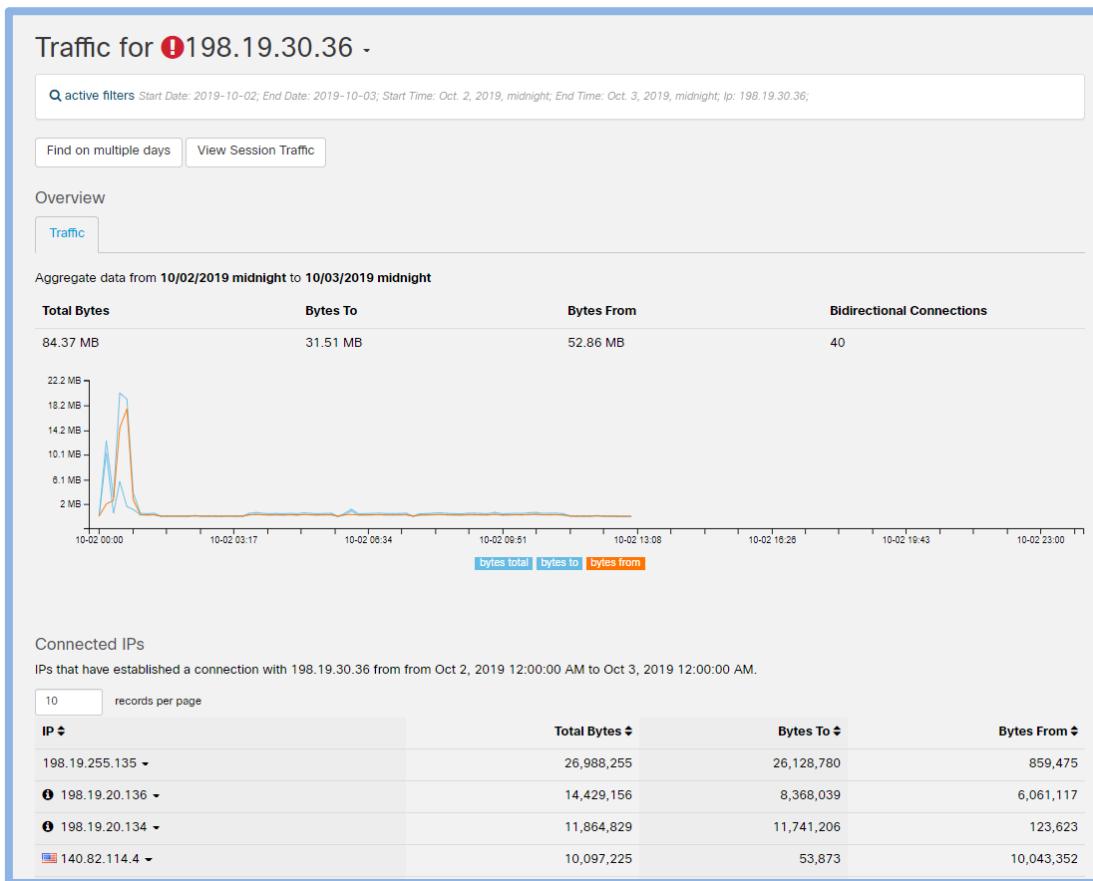
- Abnormal User** | Normal priority
A user session was created on an endpoint that does not normally see sessions with this user. This alert requires 36 days of history.
- Amplification Attack** | Normal priority
This device sent traffic with a profile that suggests participation in an amplification attack. This alert requires 0 days of history.
- Attendance Drop** | Low priority
Device is normally active for most of the day, but its activity dropped across multiple profiles (e.g., SSH Server, FTP Server). This alert requires 14 days of history.
- AWS API Watchlist IP Hit** | Normal priority
AWS API was accessed from an IP on a watchlist. This alert requires 10 days of history.
- AWS Config Rule Violation** | Normal priority
An AWS Config rule was violated. This alert requires 0 days of history.
- AWS Console Login Failures** | Normal priority
A user tried and failed to log in to the AWS Console several times. This alert requires 0 days of history.
- AWS Inspector Finding** | Normal priority
AWS Inspector reported a high-severity finding for the device. This alert requires 0 days of history.
- AWS Lambda Invocation Spike** | Normal priority
A Lambda function was invoked a record number of times. This alert requires 14 days of history.
- AWS Multifactor Authentication Change** | Normal priority
Multifactor authentication was removed from a user account. This alert requires 0 days of history.

4. Let's look more at our workstation, type the IP address of Wkst1 in the search window, by selecting the magnifying glass in the upper right hand of the portal and typing in **198.19.30.36**.

Figure 56. Search Window

The screenshot shows the Cisco dCloud interface. At the top, there are navigation links: Dashboard, Alerts (with 7 notifications), Observations, and Models. A search bar contains the IP address 198.19.30.36. Below the search bar, a message says "Gathering Data | 15 of 36 days gathered". The main title is "Traffic for 198.19.30.36 -". A filter bar indicates "active filters Start Date: 2019-12-06; End Date: 2019-12-07; Start Time: Dec. 6, 2019, midnight; End Time: Dec. 7, 2019, midnight; Ip: 198.19.30.36;". Buttons for "Find on multiple days" and "View Session Traffic" are present. On the left, under "Overview", the "Traffic" tab is selected. The overall interface is light blue and white.

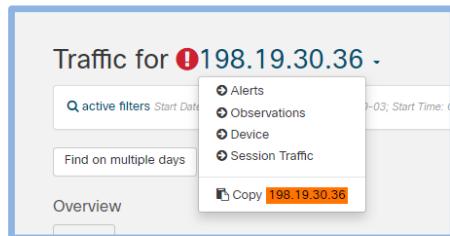
5. You will see a summary of the recent IP connectivity. View the top Connected IPs and Ports.

Figure 57. Host Traffic Report

6. Next, we will look at the Observations for this machine. Use the black triangle to pivot to Observations.

For this host you should see some initial observations such as watchlist hits and remote access connections, this will continue to grow as we collect more traffic.

Figure 58. Observations Pivot



7. Check to see if there are any alerts for Wst1. Go to the [Alerts menu](#) in the Stealthwatch Cloud portal to see if any alerts have published. Likely you will see one called “User Watchlist Hit” for the interaction between the workstation and the TOR network, soon you should also see one called “Internal Port Scanner” that will have details on the recon file we initiated earlier. If you don’t see them, then it could be still be a delay in processing. Continue to look back at the alerts.

Figure 59. Alerts Menu

Alerts			
Search...		Status	Tags
17 open alerts sorted by newest			
User Watchlist Hit wkst1.dcloud.local		2 hours ago	70
#168			
Internal Port Scanner wkst1.dcloud.local		2 hours ago	
#383			

Figure 60. Watchlist Alert

! User Watchlist Hit - wkst1.dcloud.local -

Status	Open
ID	168
Description	Device exchanged traffic with an IP address on a user-supplied watchlist, or attempted to resolve a domain name on a user-supplied watchlist. (Watchlists: Tor Traffic)
Updated	Oct 2, 2019 4:50:00 PM
Created	Sep 27, 2019 1:40:00 PM
IPs at the time of alert: 198.19.30.36	
Assignee	Nobody
Tags	
<p>After reviewing an alert, closing it will let the rest of your team know it's been resolved. In addition, closing alerts sends important feedback.</p> <p>This alert was generated using user-supplied data. You can manage watchlists from the watchlists configuration page.</p>	
<input checked="" type="button"/> Close Alert	

Supporting Observations

Watchlist Interaction Observation [🔗](#)

Device communicated with an IP address that is on a watchlist (either explicitly or implicitly via a domain name).

Time	Device	Watchlists	External IP	Domain	in	out
10/2/19 4:40 PM	wkst1.dcloud.local	Tor Traffic	217.182.50.220		4,153,203	874,952
10/2/19 4:30 PM	wkst1.dcloud.local	Tor Traffic	217.182.50.220		104,264	117,784
10/2/19 4:00 PM	wkst1.dcloud.local	Tor Traffic	104.244.79.75		27,695	13,021
10/2/19 4:00 PM	wkst1.dcloud.local	Tor Traffic	217.182.50.220		5,509,378	1,440,235

Open the User Watchlist hit alert, investigate the following sections within the Watchlist alert for **wkst1.dcloud.local** as shown below.

1. You will notice the Supporting Observations or “evidence” for why the alert was fired. As this host continues to communicate with TOR, the IP flows will continue to update.
2. Users may have several Watchlists that are active, the Observation details will reference the specific list that was defined. The external IP will show the flag of the country that it was Geo-coded to. Additionally, the Observation will summarize the traffic in 10-minute periods.
3. Click on the time-stamp to see more details on the supporting flows.

4. As part of the Alert workflow, users can add comments. Add a comment for the User Watchlist Alert. These will remain attached to the alert, alerts are kept in the Stealthwatch Portal as long as the service is active.

Figure 61. Alert Comment

The screenshot shows a 'Comments' section within a web-based interface. At the top, there is a header with the word 'Comments'. Below the header, there is a list of existing comments. The first comment is displayed in a box with a grey background and white text:
Someone talk to this employee. This is not permitted!!!!
- By john.heintz@obsvrl.com on Oct 2, 2019 7:18:51 PM
View 70 additional updates

Below the comment list is a large, empty text area for new comments, labeled 'Comment on this alert.' A blue 'Comment' button is located at the bottom left of this area.

5. If the port scanner alert has triggered, open it and look at this Observations as compared to the Watchlist alert. Click the timestamp to see all the flows that were used for that alert. Try closing the alert to see how Stealthwatch Cloud prompts for user feedback so we can ensure alerts provide value to our customers. If it has not generated yet, come back after the next lab.

Figure 62. Internal Port Scanner

The screenshot shows the alert details for an Internal Port Scanner. The alert ID is 383, and it was created on Oct 2, 2019, at 4:09:36 PM. The status is Open. The description indicates a port scan was started on a device internal to the network. The IP at the time of the alert was 198.19.30.36, and the hostname was wkst1.dcloud.local. There is no assignee, and the alert has a tag. A note says "After reviewing an alert, closing it will let the rest of your team know it's been resolved. In addition, closing alerts sends important feedback." A green button labeled "Close Alert" is present. Below this, the "Supporting Observations" section shows a table of scanned ports. The table includes columns for Time, Device, Scan Type, CIDR Range, Count of ports scanned, Port Ranges, and Time Window. One entry shows a scan from 10/2/19 4:05 PM by wkst1.dcloud.local (internal) against targets 10.201.0.0/24, 198.19.20.1/32, and 198.19.20.141/32, resulting in 7 common targets over a 4m 1s window. A CSV download link and a page number indicator (1 of 1) are also visible.

Figure 63. Alert Feedback

The dialog box is titled "Feedback". It asks "Was this alert helpful?" and provides a note: "This provides feedback to us. It doesn't directly change our alerting criteria." Two buttons, "Yes" and "No", are shown. The next section, "Snooze this alert?", lists the type (Internal Port Scanner), scope (Source), and value (wkst1.dcloud.local). It also includes a dropdown for "Don't snooze" and a note: "Don't show the alert matching the above criteria for a period of:". At the bottom are "Cancel" and "Save" buttons.

Summary

Within this test drive you learned:

- How to investigate an alarm
- How to investigate a host
- How Observations are used to detect network or user events and create alerts
- How to review Stealthwatch for alert and Observations

Lab 2: Historical Traffic Analysis to Identify Threats from Suspect Countries

Business Objectives

Threats are hiding in legitimate network traffic through common web browsing or through ports and applications that are trusted within firewall rules and on the endpoint. One way to identify these threats is to account for all network traffic entering and leaving the organization to the Internet.

Once this visibility is collected, retrospective analysis over this long-term history can be performed to identify what should not exist. Through this visibility and retrospection, detection of threats will be improved along with being able to improve enforcing network segmentation.

Test Drive Objectives

Within this test drive you will gain an understanding of the importance of accounting for all traffic entering and leaving your organization to the Internet to identify threats hidden within trusted connections.

Test Drive Requirements

- Stealthwatch Cloud Portal

Test Drive Outline

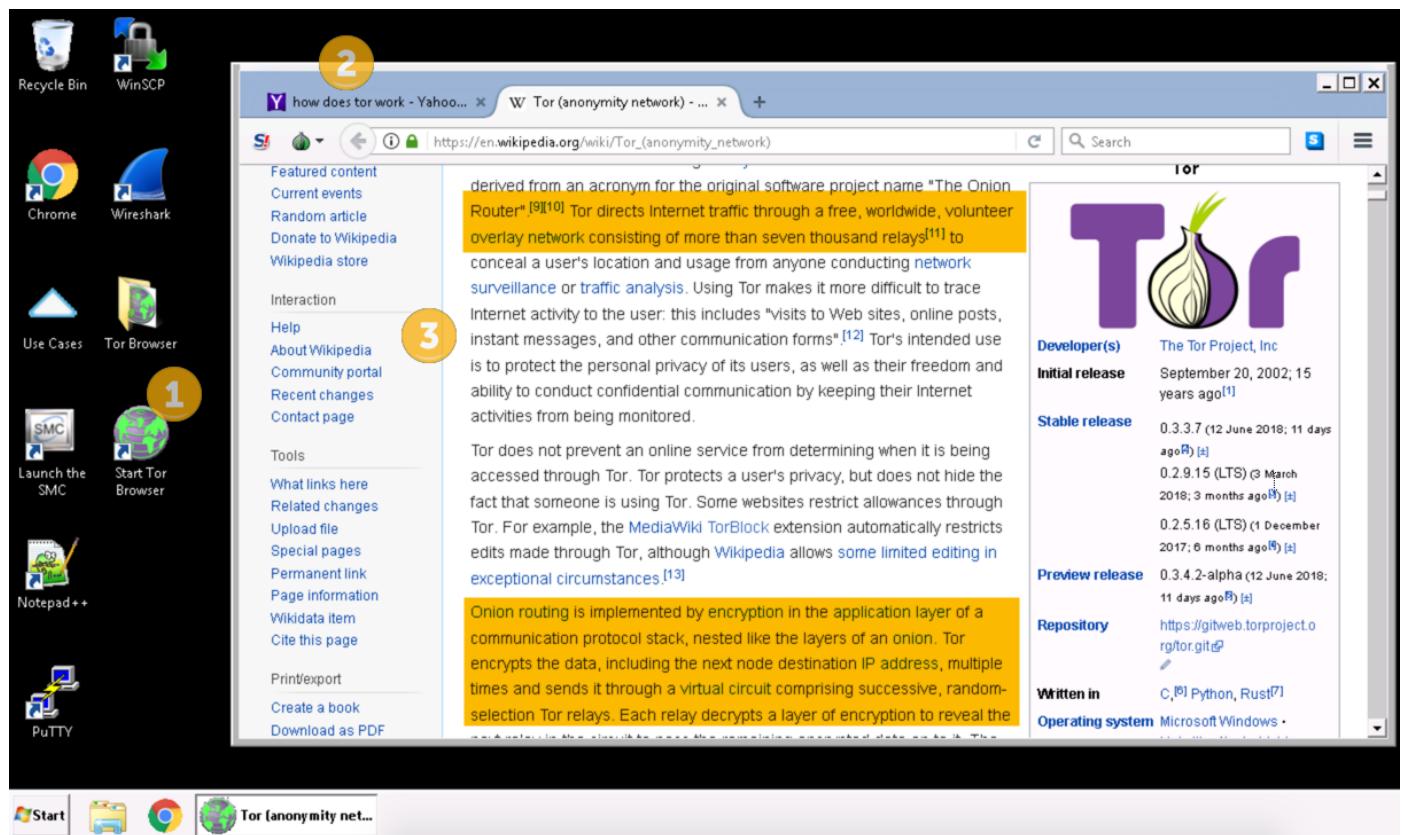
- Task 1. Generate traffic to random countries.
- Task 2. Identify traffic to random countries.
- Task 3. Identify what alerts are activated for high risk countries

Task 1: Generate traffic to random countries

Within this section you will generate random traffic that is trusted from an installed application over common ssl web traffic.

1. Click **Start Tor Browser** from the desktop of the remote desktop Workstation 1.
2. Navigate to yahoo.com to (if you are redirected scroll down to the bottom and accept the Yahoo privacy agreement) begin generating web traffic and click on a few articles. Yahoo.com is being recommended as the search engine as it contains many widgets that generate more web connections to different sites. After browsing through a few articles to generate traffic, search for “[how does tor work](#)”.
 - a. **Note:** Browsing with TOR can be very slow by nature
3. Open and read the Wikipedia article shown below on how the Tor network works.

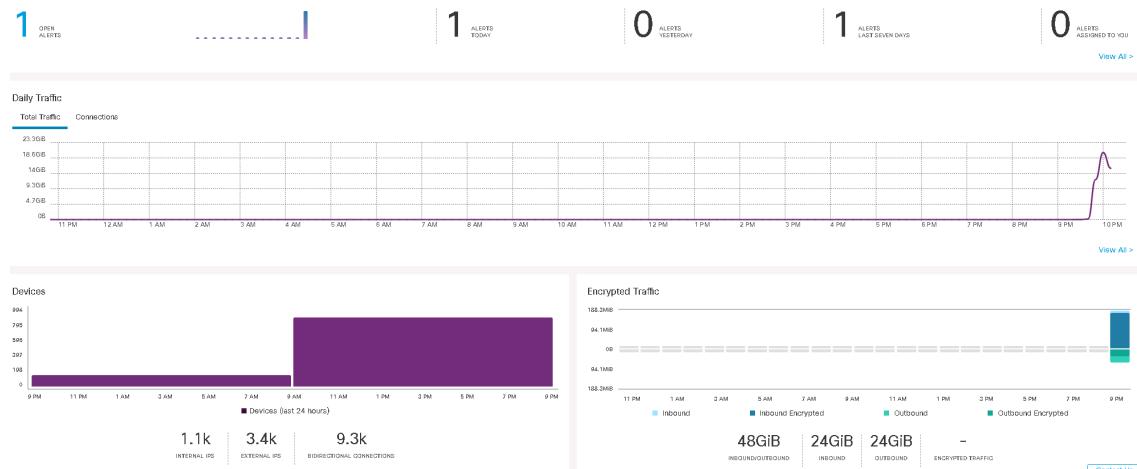
Figure 64. Search within the Tor Browser



Task 2: Investigate traffic to random counties

Within this lab you will learn how to view all countries your Workstation 1 has connected to.

1. Open the Stealthwatch Cloud portal and login
2. Select Dashboard, then your portal will start displaying details about the network activity, such as traffic, connections, encrypted traffic, etc.



- Stealthwatch Cloud Geo-locates any IP that a device communicates with, it will track the traffic to countries you designate as high risk. This page summarizes the country activity.

Figure 65. Country Heat Map



- Select the settings icon, then Alerts, then Configure Alert Priority. Do a Ctrl+F to run a search on this page for “Geographic”, this will list any Geo based alerts. Three alerts are associated with the Country Watchlist.

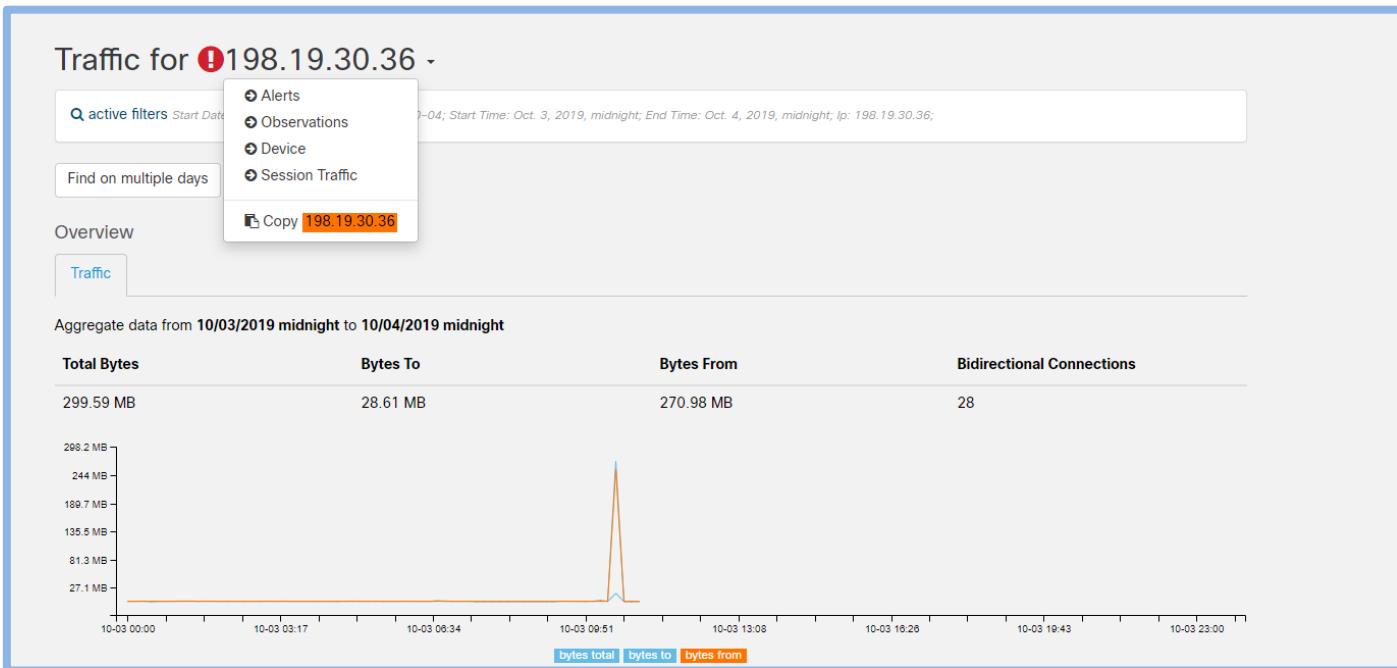
Figure 66. Country Watchlist Alerts

Protocol Violation (Geographic) | Normal priority ⓘ
Device tried to communicate with a host in a watchlisted country on an illegal protocol / port combination (e.g., UDP on port 22). This alert requires 0 days of history.

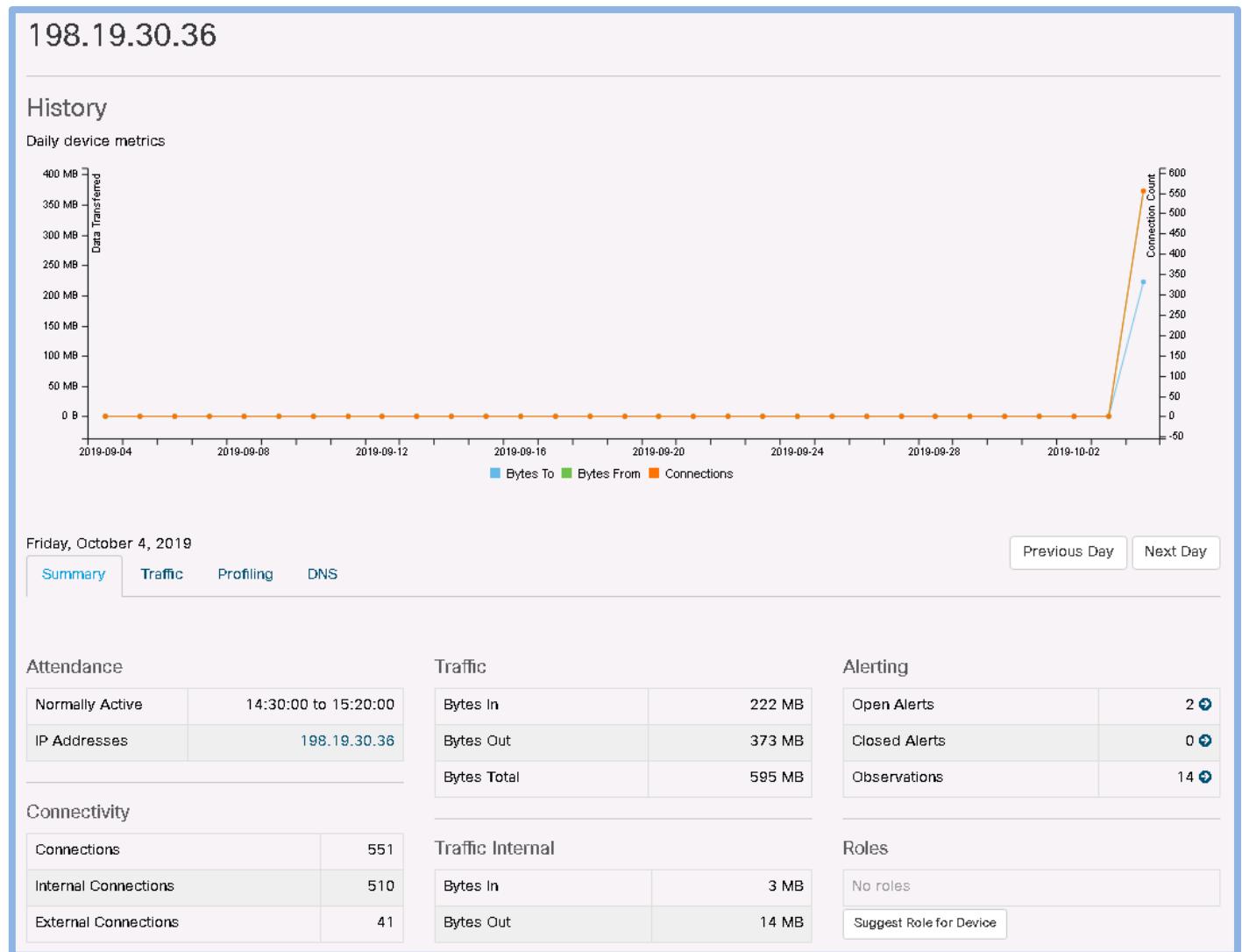
Remote Access (Geographic) | Normal priority ⓘ
Device has been accessed from a remote host in a watchlisted country. This alert requires 0 days of history.

New Long Sessions (Geographic) | Normal priority ⓘ
Device has established a long-lived connection with a host in a watchlisted country. This alert requires 2 days of history.

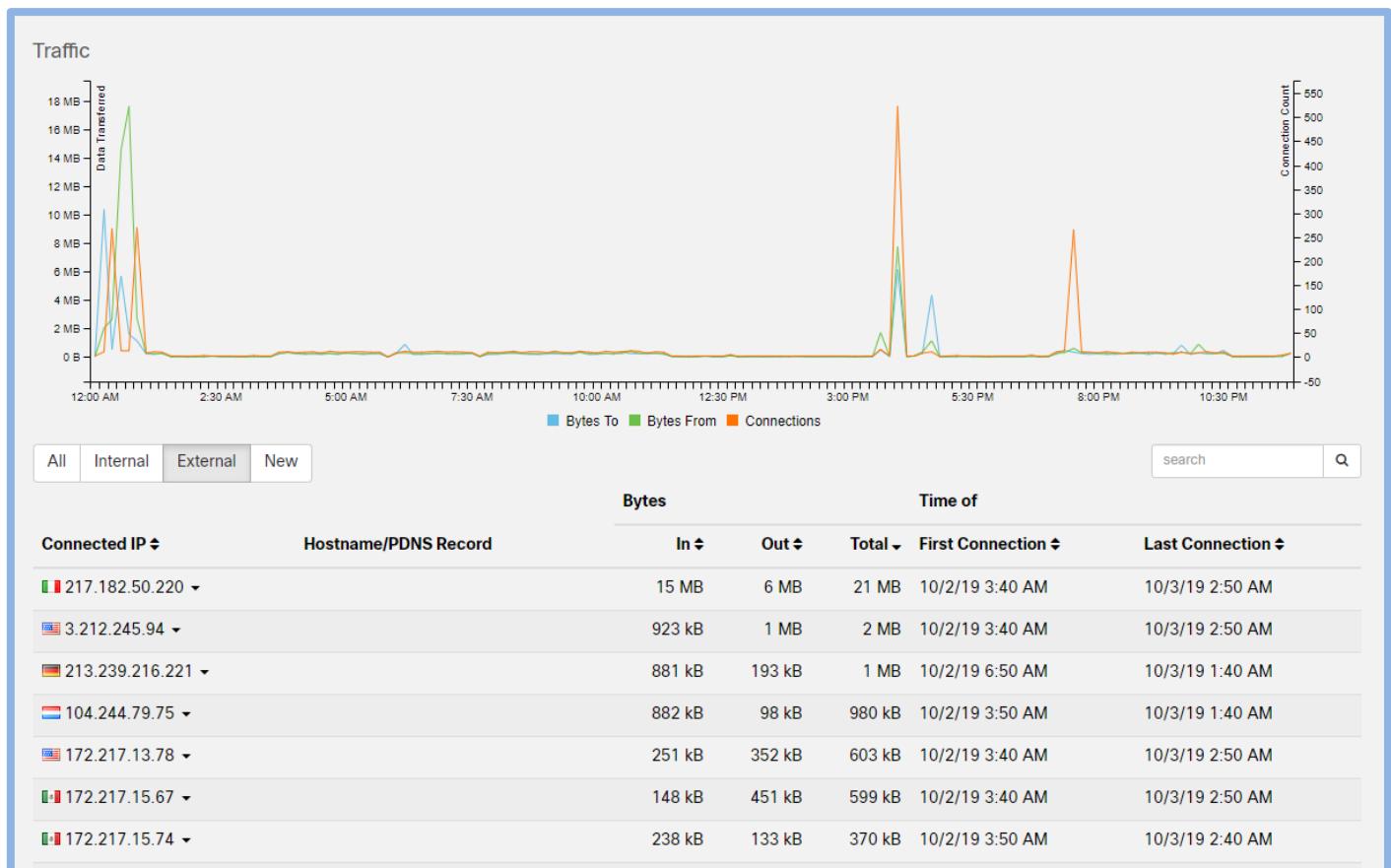
5. Let's now look the countries that WKST1 has communicated with. Select the **hour glass** to search for IPs in the portal. Enter 198.19.30.36 to pull our workstation.
6. Select the **triangle** next to the IP address and then **Device**



7. This initial device page summarized connectivity for a given day such as Internal and External Connections, Traffic Profiles sorted by byte count, etc. Since this is a new system there is not history prior to today. We also don't have a role detected yet since we have not seen enough traffic to say for sure what kind of roles the device is part of.

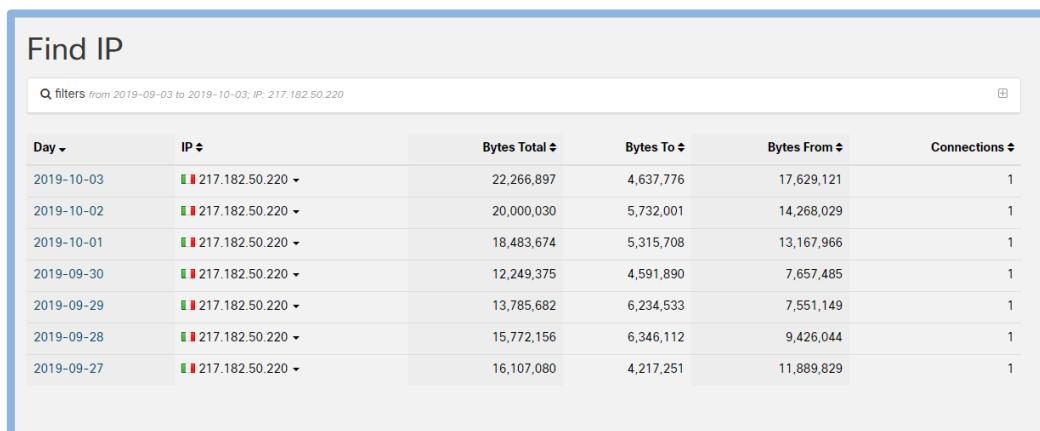
Figure 67. Device Summary View

8. Next select the traffic tab. This page will show detail about the internal and external communication for a specific day. Select External to see all traffic to IPs not listed as local subnets. You can sort by Bytes and Connection time.



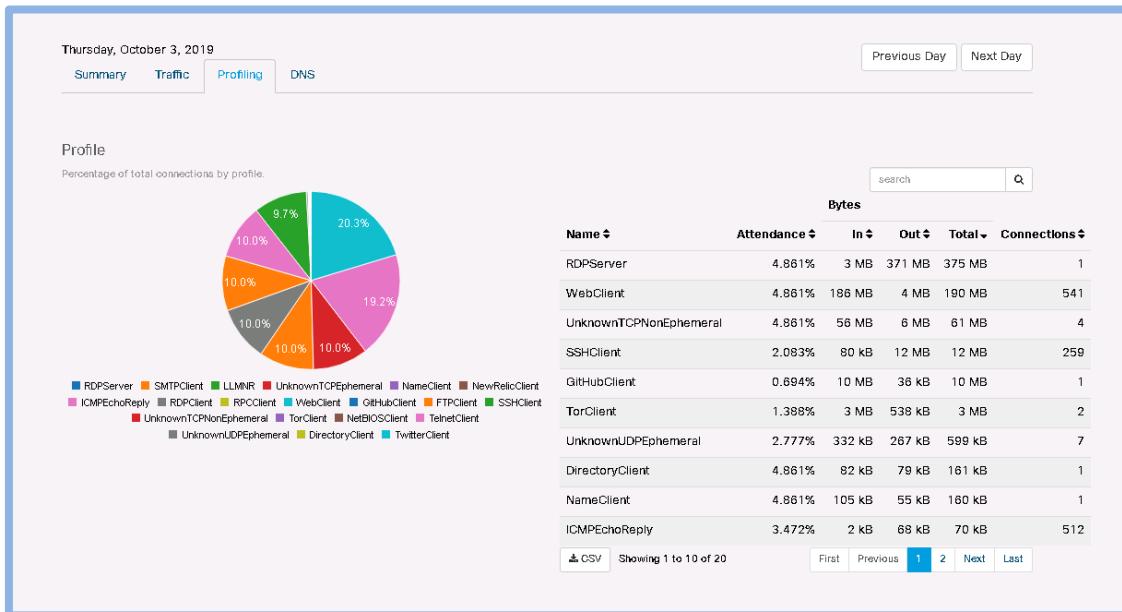
- To see more details and options about an external host, select the triangle next to the IP address. For example, you can see all traffic to that IP across any IP address in the portal by selecting find IP on multiple days.

Figure 68. Traffic Report for External Host



10. Select Profiling which is the next tab in the device view. This shows the connections by type of application, for Wkst1 the top application by traffic is RDPServer but since it only has one connection it a small part of the pie chart. This is another quick way to visualize day by day the behavior of a machine to see what has changed.

Figure 69. Traffic Profiles



11. Select Observations, then types, scroll down until you find Geographic Watchlist Observations, click the arrow next to it. As flows are processed each flow that matches a country on the watchlist will be listed here. This may be empty initially as the system is new, check in 24 hours to see how many flows are to high risk countries.

Figure 70. Wkst1 Observations

Observations				
Geographic Watchlist Observation		Device communicated with watchlisted geographic region.		
Time	Device	External IP	Country	
10/3/19 9:50 AM	10.201.3.106	4.27.255.126, 8.9.23.204, 8.12.218.126, 8.27.244.253, 50.56.217.21, 54.243.222.88, 64.4.11.25, 64.14.29.85, 64.14.29.200, 64.94.107.35, 64.94.107.41, 65.54.81.51, 65.54.81.173, 66.235.134.217, 66.235.142.24, 67...	United States	
10/3/19 9:50 AM	10.201.3.106	12.129.199.104	Germany	
10/3/19 9:50 AM	10.201.3.106	178.255.83.1	United Kingdom	
10/3/19 9:50 AM	10.201.3.106	199.7.59.72	France	
10/3/19 9:50 AM	10.201.3.84	23.62.194.110, 23.62.207.144	France	
10/3/19 9:50 AM	10.201.3.84	65.55.200.138, 69.171.229.25, 69.171.234.34, 74.125.137.139, 74.125.140.93, 74.125.140.100, 74.125.140.102, 74.125.140.113, 74.125.140.138, 74.125.140.139, 74.125.140.190, 74.125.229.160, 74.125.229.174, 96.17.32.170, 143.127.102.4...	United States	
10/3/19 9:50 AM	10.201.3.84	173.194.39.98	Germany	
10/3/19 9:50 AM	10.201.3.32	17.158.10.25, 17.158.10.36, 17.158.10.37, 17.158.10.43, 17.158.10.46, 17.167.136.33, 17.172.232.146, 50.16.216.36, 50.19.240.2, 63.250.192.40, 64.12.24.31, 64.12.104.176, 64.12.152.13, 64.236.116.15, 65.54.48.88, 66.22...	United States	
10/3/19 9:50 AM	10.201.3.32	23.8.0.107	Germany	
10/3/19 9:50 AM	10.201.3.144	17.172.232.193, 31.13.77.42, 31.13.77.58, 66.220.158.16, 69.31.74.26, 69.31.74.73, 69.31.74.82, 69.171.224.42, 69.171.237.24, 69.171.237.40, 69.171.246.16, 74.125.120.94, 74.125.127.17, 74.125.127.100, 74.125.127.101	United States	

Summary

Within this lab you learned:

- The importance of accounting for all traffic to and from the Internet
- How to perform network retrospection to suspect countries
- How to detect research traffic for a host or external IP address.
- What alerts are linked with high risk countries.

End of Lab: Please pause here.

Insider & Advanced Threat Detection



I plan to leverage my access for a side hustle.

Goals

- ① If I am being deliberate, my goal may be to hurt my company or to personally gain financially or otherwise
- ② Steal HR records to get everyone's salary to better negotiate my position
- ③ Exploit a flaw in financial software to make a financial gain from the exfiltration of data or the installation of malware

Attack Vectors

- Data Exfiltration
- Installing Malicious Software
- Exploitation of Poor Access Controls

Izzy
The Insider Threat

Google This:
 Target Breach, Anthem exfiltration, Boeing spy

Age: 18-60
Location: Global
Description: Insider threats range from careless employees (accidentally misplace laptop, uses universal passwords, etc.) to malicious employees. Insider threats can also result from compromised employee accounts.

Mitigation Techniques

- Strict and comprehensive Identification, Access and Authorization controls for all users
- Regular internal security audits/vulnerability scans
- Endpoint control systems
- Agents with comprehensive logging, tracing and alerting
- User Behavioral Analytics
- Well defined security policies and enforcement mechanisms

Expertise

Security	
NOVICE	EXPERT

Networking	
NOVICE	EXPERT

SecOps Strategy

MONITOR 	ALERT 	TRACK
Monitor for data exfiltration to the Internet or other unusual destinations	Trigger alerts for unusual relationships that do not commonly occur or are not permitted	Track anomalous network traffic such as excessive flows from an endpoint to a valuable server

Lab 3: Data Exfiltration

Business Objective

One of the most valuable assets for an organization is its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars.

Stealthwatch Cloud tracks inside and outside hosts to which an abnormal amount of data has been transferred. If a host triggers events exceeding a configured threshold, it results in an Exfiltration alarm. In this lab we do not have a baseline to compare to so we are going to simulate the traffic and check for observations that match that type of activity.

Optimally configure Stealthwatch Cloud to send alerts to a Cisco Teams room if you have access to create one.

Test Drive Objectives

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

The Suspect Data Loss security event is in the Exfiltration alarm category and based on observed flow rather than a number of default points assigned to the alarm category when the security event occurs.

When this event triggers, an inside host acting as a client has uploaded a cumulative amount of TCP or UDP payload data to an outside host, and the amount exceeds the threshold set in the policy applied to the inside host.

What does it mean when this alarm fires? A host is being used to upload more information to the Internet than is acceptable. This can be anything from someone using external backup services to maliciously exfiltrating corporate data.

Test Drive Requirements

- Stealthwatch Cloud Portal
- Any version of NetFlow from within the network
- Visibility of all host-to-host traffic from the core/distribution

Test Drive Outline

The “attacker” in this scenario will be sending a large file from the system to a host on the Internet. In the example given in this document we will use ncat, but you could also transfer a file to a web file storage system like Google Drive or Dropbox.

Ensure you are collecting full NetFlow somewhere along the path between the attacker and victim IP.

- In the following examples, the attacker IP address will be 198.19.20.36

A disgruntled employee has downloaded customer information from a database server and is now sending critical sensitive data to a destination outside of your network.

Transfer a large amount of data to your attacking system

The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your file share.

If you are using Windows and copying the file across a Windows file share, use Windows Explorer to connect from the attacker system.

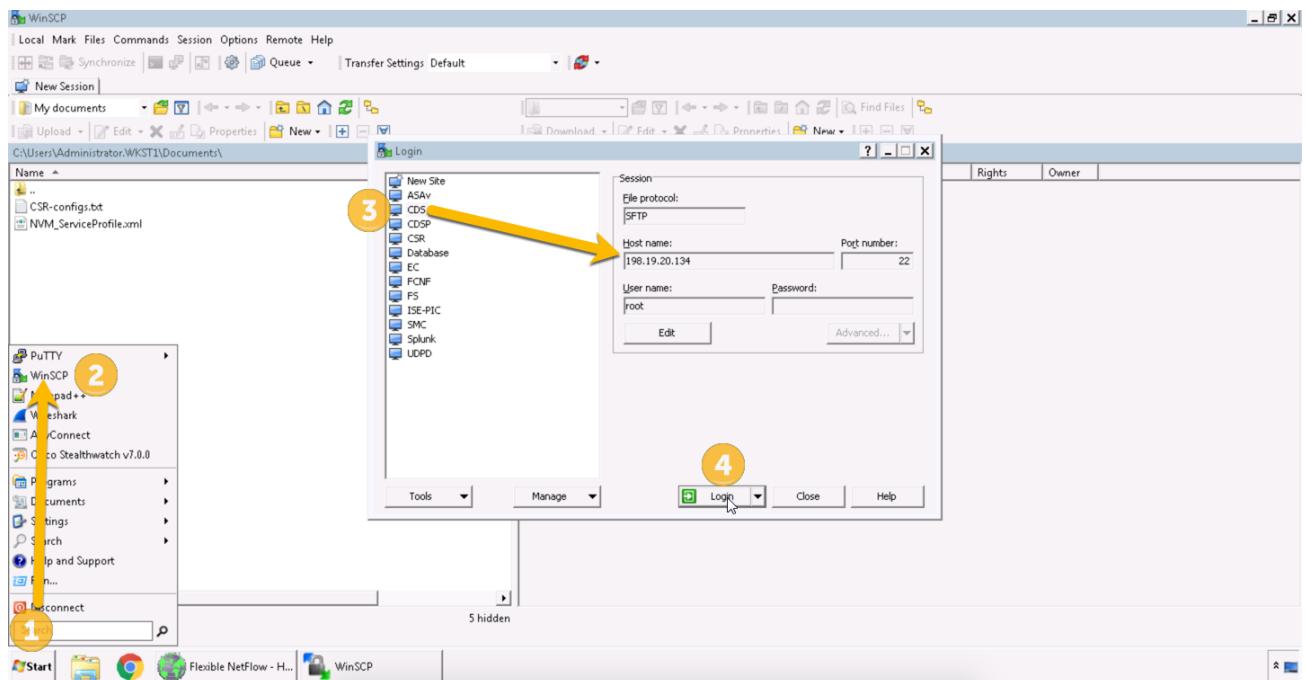
An FTP client would be used if you are connecting to a system serving files with an FTP server.

In this example, we will be transferring a 380 MB file via SCP from a database server to the Workstation 1 within dCloud.

1. Select **Start** from Workstation 1, as shown below.
2. Select **WinSCP**, as shown below.
 - a. **Note:** If an update appears, ignore the update.
3. Select **CDS**, as shown below.
 - a. **Note:** The IP address of **198.19.20.134**, the username and password are already cached for login.
4. Select **Login** and end **C1sco12345** for the password.

NOTE: If prompted with a certificate warning in WinSCP just click OK and continue.

Figure 71. Login WinSCP



5. Locate the file or files that you will be transferring. In this case it is the **encrypted-customer-DB** and transfer it to your downloads folder on the Workstation 1.
6. Initiate the transfer to the attacker system
7. Close WinSCP

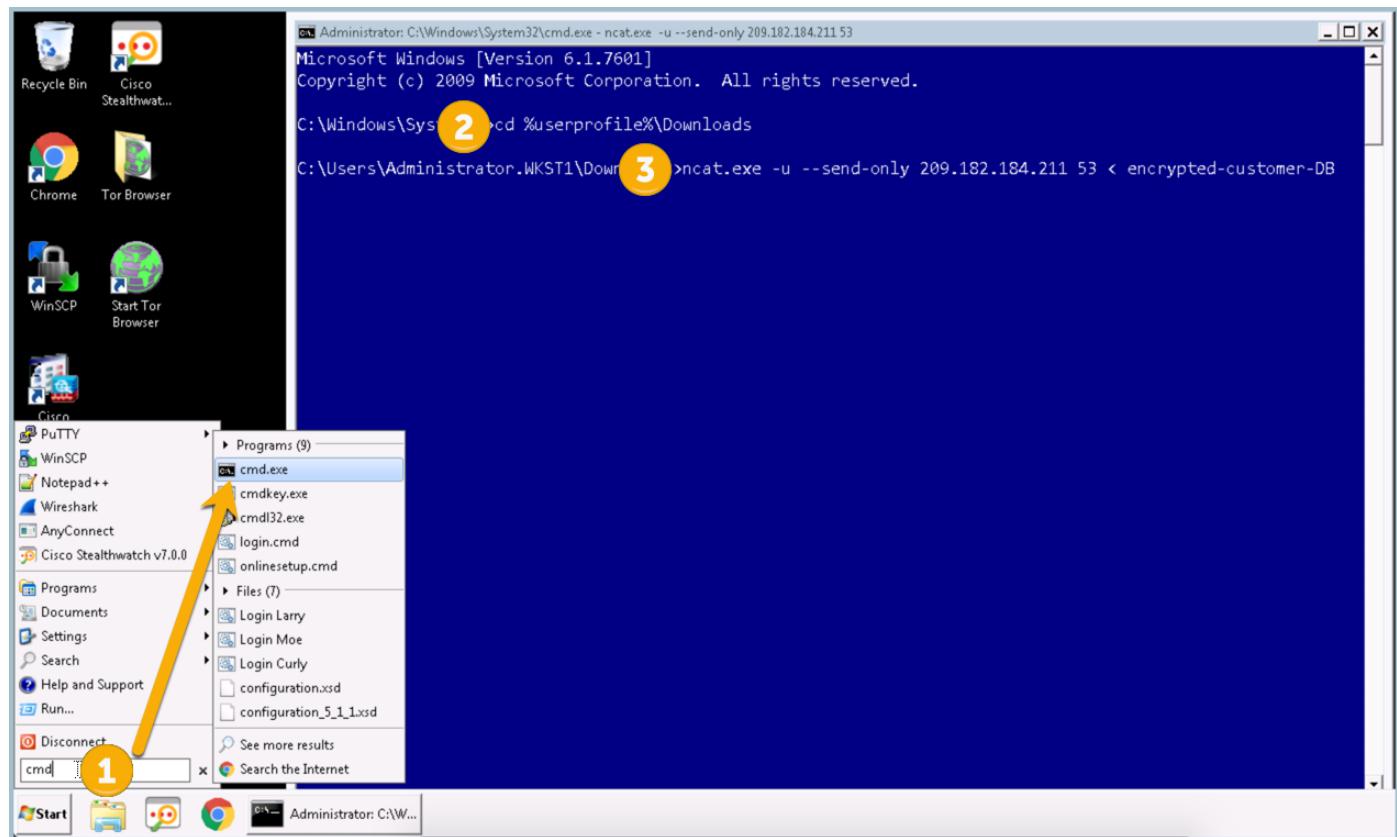
Transfer a large amount of data from your attacking system

The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your external file share.

An FTP client would be used if you are connecting to a system serving files with an FTP server, or you could use a web browser to transfer the file to a service such as Google Drive or Dropbox.

Transfer the 380 MB file to a remote host using ncat.

1. From Workstation 1, open **cmd.exe** to bring up the command prompt in Windows as illustrated below.
1. Change the directory to the Downloads directory using the change directory command: **cd %userprofile%\Downloads** in command prompt as shown below.
2. Enter **%u** the command prompt as illustrated below. Ncat.exe is used to stream the file to an external IP address. The –u option uses UDP as the protocol and 53 is the port.

Figure 72. ncat

Note: This could take up to several minutes to finish transferring. Be sure to check the Security Insight Dashboard for the Exfiltration alarm increasing.

While the tool is executing take a look at the following article:

https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.e97851379584

Move on to the next lab, we will review the transfer activity later after it has been processed.

End of Lab: Please pause here.

High Risk Application Detection

Lab 4: Detecting Internal Telnet Traffic

Business Objective

Many organizations prohibit the use of Telnet on the network. It is an unsecure protocol because it transfers data in clear text, introducing the risk of exposing login credentials to an attacker. Telnet can open an organization up to data loss. Mainframes and financial systems that contain customer information often run Telnet, leaving them vulnerable to network monitoring attacks.

Stealthwatch Custom Security Events can be created to alarm on unauthorized Telnet communications or other unwanted applications against a group of hosts.

Test Drive Objective

Security events contribute index points to alarms. Alarms are grouped into Alarm Categories.

The Policy Violations Alarm Category is a Custom Security event created to report on policy violations or unwanted communications in an organization.

Test Drive Requirements

The Stealthwatch system configuration minimum requirements are:

- Visibility of all host-to-host traffic from the core/distribution
- StealthWatch Cloud

Test Drive Outline

The “attacker” in this scenario will attempt to connect to a database using Telnet.

StealthWatch Cloud can use tripwires configured inside the network to catch unauthorized local and remote access. We will create a customer watchlists to detect this traffic.

Create an Internal Connect Watchlist to Detect Telnet Traffic Internally

In this lab, we set up a Custom watchlist to watch for telnet traffic to the 192.168.30.0/24 subnet, Telnet uses port 23/tcp. We could also create permit rules, these are similar to an ACL in that we can say some traffic is permitted, for example a legacy application that must use Telnet,

1. Open the Stealthwatch Cloud portal
2. **Select** Settings > Alerts, Configure Watchlists, Internal Connection Watchlist

Figure 73. Internal Connection Watchlist

The screenshot shows the 'Watchlist Config' interface. At the top, there's a navigation bar with tabs: ' IPs and Domains', 'Expired IPs and Domains', 'Third Party Watchlists', 'Expired Third Party Watchlists', and 'Internal Connection Watchlists'. The 'Internal Connection Watchlists' tab is selected. Below the tabs, the title 'Internal Connection Watchlists' is displayed. A message 'This list is empty.' is shown above a 'CSV' download button. The main area contains a table with columns: 'Allowed?', 'Name', 'Source Subnet', 'Source Ports', 'Destination Subnet', 'Destination Ports', and 'Reason'. There are no rows in the table.

Allowed?	Name	Source Subnet	Source Ports	Destination Subnet	Destination Ports	Reason
This list is empty.						
CSV						

Add Connection

Name	<input type="text" value="Name"/>
Source IP*	<input type="text" value="192.168.1.0"/>
Source Block Size*	<input type="text" value="24"/>
Source Ports	<input type="text" value="Comma separated ports (22) or port ranges (22-24)."/>
Destination IP*	<input type="text" value="192.168.2.0"/>
Destination Block Size*	<input type="text" value="32"/>
Destination Ports	<input type="text" value="Comma separated ports (22) or port ranges (22-24)."/>

Complete the following steps:

1. Enter Name: **CSE: Telnet Traffic**
2. Source IP: **198.19.30.0**
3. Source Block Size: **24**
4. Source Ports: **23**
5. Destination Port IP: **0.0.0.0**

6. Destination Block Size **0**
7. Destination Ports: **0 - 65535**
8. Reason: **Telnet not permitted internally**
9. **Click Add**

Figure 74. Watchlist Config

Enable the Telnet Server on Wkst1

In this task, we will enable the telnet server on the Wkst1 to show how easy it is for end users to expose risk to the organization.

Make sure the Telnet service is running:

1. From the Remote Desktop Workstation select the Start button and search for **Services**
2. Open **Services**
3. Scroll down and **double click** on **Telnet**
4. Make sure the **Startup Type** is set to **Automatic** and select **Apply**
5. Select **Start** if the service is not running
6. Select **Ok**

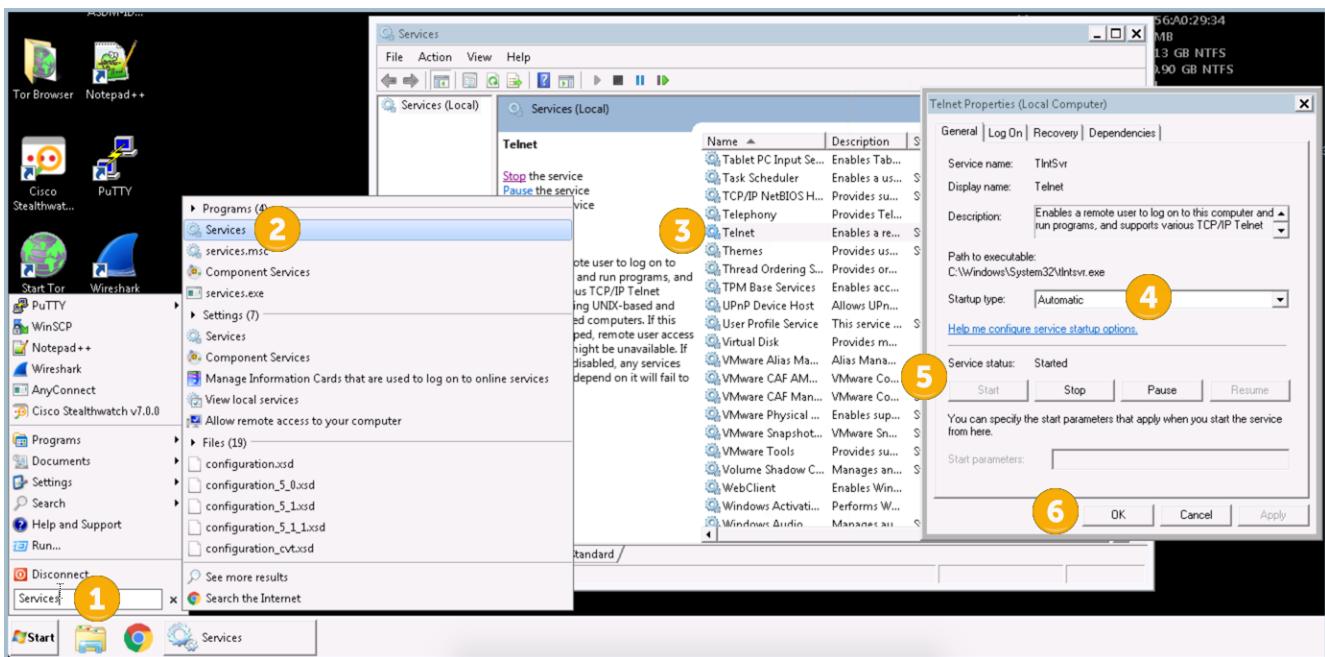
Figure 75. Install Telnet

Make sure the Telnet service is running:

1. From the Remote Desktop Workstation select the Start button and search for **Services**
2. Open **Services**
3. Scroll down and **double click** on **Telnet**
4. Make sure the **Startup Type** is set to **Automatic** and select **Apply**
5. Select **Start** if the service is not running

6. Select Ok

Figure 76. Start Telnet

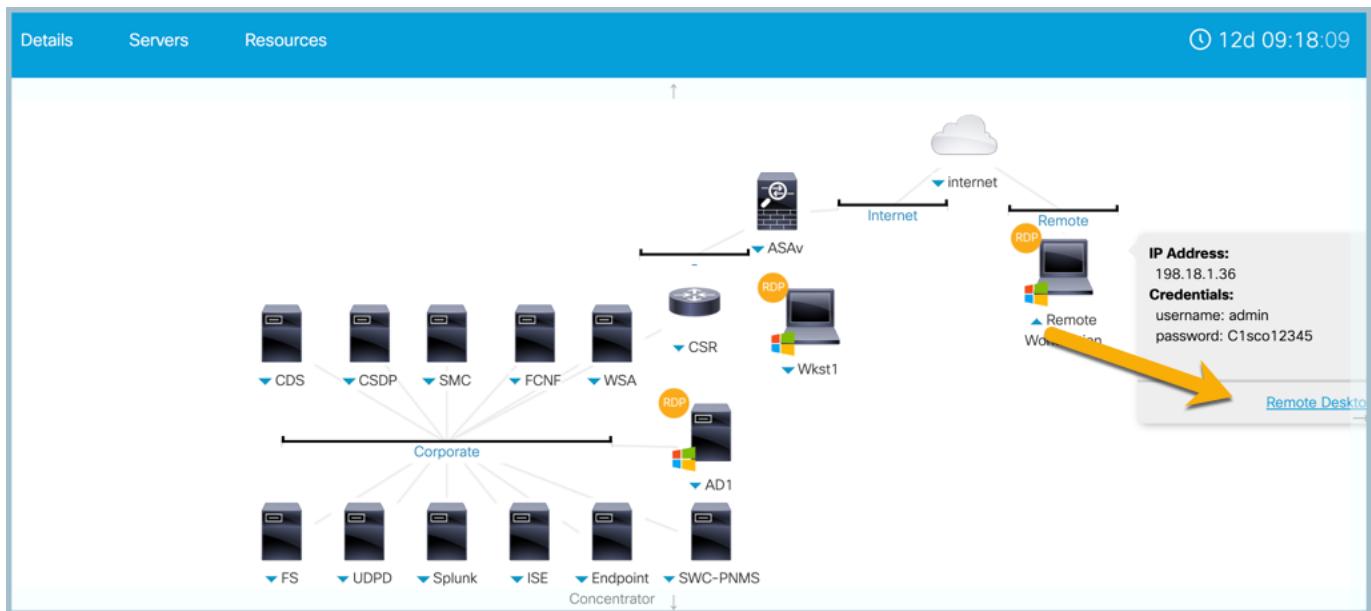


Connect to Server over Telnet from Remote VPN Workstation

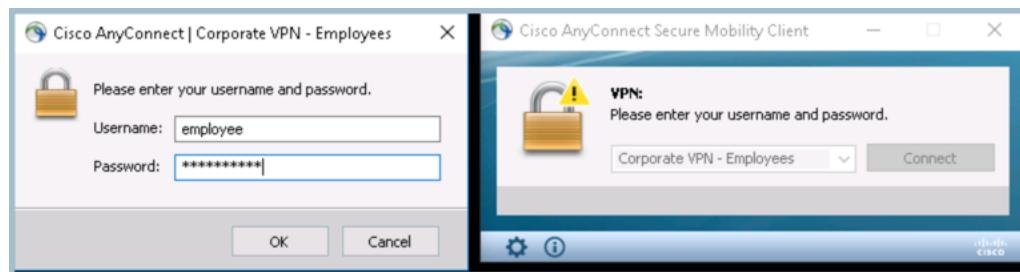
In this task, we will use the Remote Workstation to connect to the Telnet server.

1. Open <https://dcloud.cisco.com> in a web browser and select **My Hub**
2. Select **View** for the current Cisco Stealthwatch 7.1 & ETA Test Drive Lab v2.2.
3. Select the **Remote Desktop hyperlink** under Remote Workstation as illustrated below.

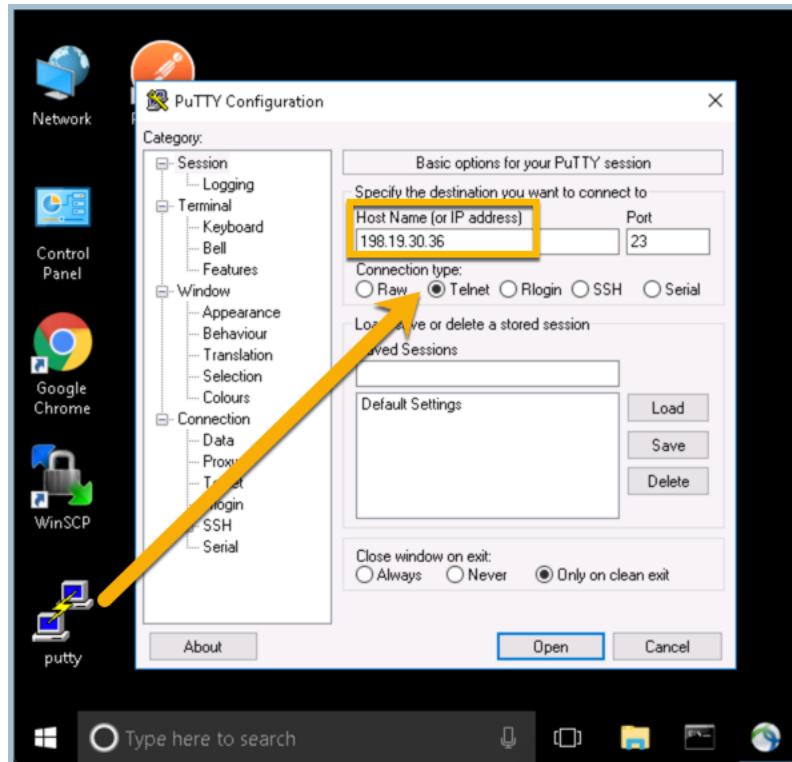
NOTE: If you have trouble connecting to the Remote Desktop you may need to Reboot the workstation from the Servers utility.

Figure 77. Remote VPN

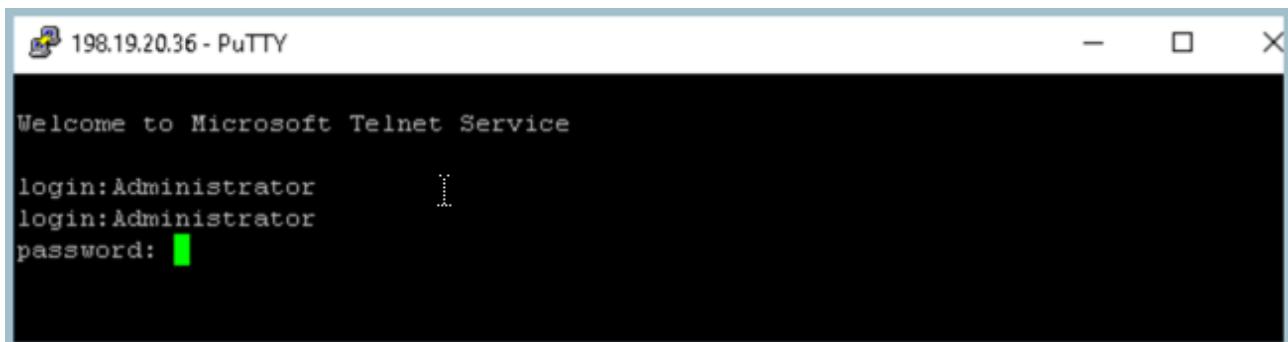
4. If prompted to login the username is admin and password C1sco12345.
5. **Launch** AnyConnect (if it does not automatically display; it is located in the services menu in the bottom right corner) and **Login** to Cisco AnyConnect Corporate VPN – Employees profile with username **employee** and password **C1sco12345**

Figure 78. AnyConnect

6. Launch **Putty** from the desktop and enter **198.19.30.36** in the host name field
7. Select **Telnet**

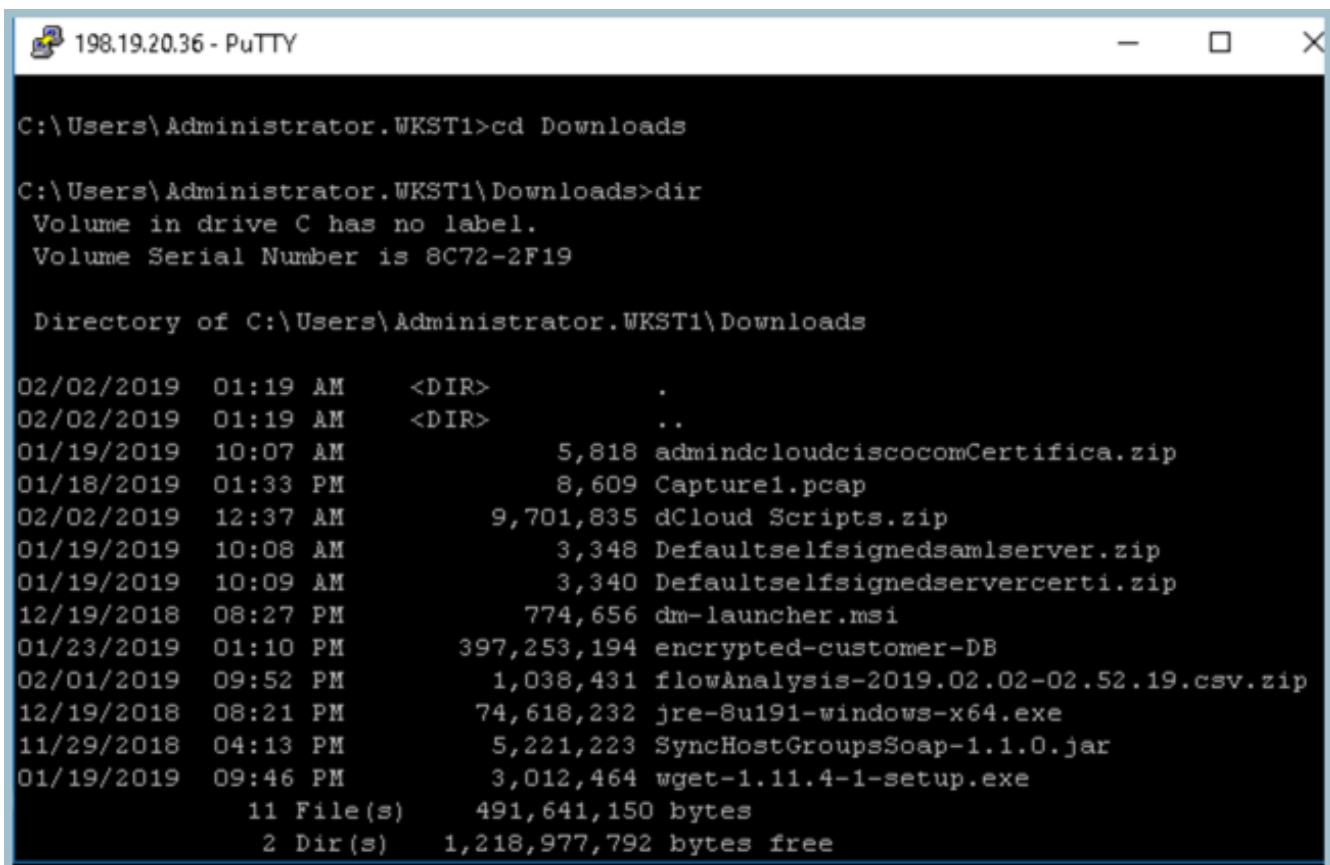
Figure 79. Putty

8. Press the **Enter** key to begin logging into the Telnet session use username **Administrator** with password **C1sco12345** as illustrated below

Figure 80. Telnet

9. Run a few commands to validate you have a successful Telnet session into 198.19.30.36. Start with **ipconfig** to verify the IP address. Next enter **cd Downloads** and **dir** to list the directory as illustrated below. Type **exit** to drop the Telnet session and close the remote desktop session.

Figure 81. Talent Commands



The screenshot shows a PuTTY terminal window titled "198.19.20.36 - PuTTY". The command prompt is at the top. Below it, the user has run the following commands:

```
C:\Users\Administrator.WKST1>cd Downloads
C:\Users\Administrator.WKST1\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 8C72-2F19

Directory of C:\Users\Administrator.WKST1\Downloads

02/02/2019  01:19 AM    <DIR>      .
02/02/2019  01:19 AM    <DIR>      ..
01/19/2019  10:07 AM      5,818 admindcloudciscocomCertifica.zip
01/18/2019  01:33 PM      8,609 Capture1.pcap
02/02/2019  12:37 AM     9,701,835 dCloud Scripts.zip
01/19/2019  10:08 AM      3,348 Defaultselfsignedsamlserver.zip
01/19/2019  10:09 AM      3,340 Defaultselfsignedservercerti.zip
12/19/2018  08:27 PM      774,656 dm-launcher.msi
01/23/2019  01:10 PM    397,253,194 encrypted-customer-DB
02/01/2019  09:52 PM    1,038,431 flowAnalysis-2019.02.02-02.52.19.csv.zip
12/19/2018  08:21 PM    74,618,232 jre-8u191-windows-x64.exe
11/29/2018  04:13 PM    5,221,223 SyncHostGroupsSoap-1.1.0.jar
01/19/2019  09:46 PM    3,012,464 wget-1.11.4-1-setup.exe
               11 File(s)   491,641,150 bytes
               2 Dir(s)   1,218,977,792 bytes free
```

It will take approx. 45 minutes for Stealthwatch Cloud to get the data and analyze it to produce the Internal Connection Watchlist hit alert. Check back on Alerts after you finish the ETA section.

StealthWatch Cloud includes a built-in assessment for risky traffic such as Telnet or unauthorized DNS. You will have access to the portal until the end of the week, to see the Visibility Assessment for your portal go to ? > Visibility Assessment. You can export a copy of the data in PDF for later reference.

Visibility Assessment Beta

[Download PDF](#)

Internal Monitored Network

Modern organizations need internal visibility to understand the state of their network and its traffic. Stealthwatch Cloud continuously monitors data transferred between servers and the internet, and processes traffic flows. These metrics and others help security and network personnel quantify the hosts, systems, and resources on their network, making sure there is nothing present that they don't know about. It also helps identify critical assets, validate policies, audit and demonstrate compliance, and make better decisions based on data.

1,574	Hosts communicating within your network
3.1 TB	Internal traffic occurring on your network
134.2 GB	Traffic exchanged between your network and the internet
37.4 GB	Encrypted traffic exchanged between your network and the internet
27.9%	Fraction of encrypted traffic exchanged between your network and the internet
1	Active sensors
42,984,082	Flow records analyzed

External SMB Risk

Threat actors frequently target organizations by exploiting the Server Message Block (SMB) protocol to gain control of hosts. SMB is commonly used in many organizations and attackers use it to mask their activities on the network. Targeted destructive malware such as Conficker exploit vulnerabilities in SMB to deploy proxy tools, backdoors, and destructive tools. Stealthwatch Cloud monitors for hosts with many SMB sessions with hosts outside the network, which is consistent with worm propagation.

No External SMB traffic found in the past 30 days.

DNS Risk

DNS servers are critical to normal network function as they translate URLs to IP addresses. Many organizations utilize specific DNS servers to safeguard their network and enforce policies. When a host is found to be using an unauthorized DNS server, it could indicate malicious activity or policy violation. Malware may change a host's DNS server to forward request to sites used for phishing or exploit delivery. Likewise, network users may utilize unauthorized DNS servers to access web resources forbidden by internal policies.

Unauthorized DNS servers can:

Review Stealthwatch Observation for Unusual DNS activity

Earlier we transferred a large file using port 53 (DNS), Stealthwatch Cloud uses entity modeling and baselining to detect behavior deviations, since the portal we are using is new there is not enough of a baseline yet for some of the detections to generate. To see the flagged DNS activity, go to the Observations menu, the select [By Types](#), scroll down to [Unusual DNS Resolver](#) and [Unusual Packet Size](#) Observations. Notice the DNS transfer we did earlier.

Unusual DNS Resolver Observation (39)

Device communicated with an unusual DNS resolver.

Unusual Packet Size Observation (0)

Device sent or received packets that are unusually sized for the given profile.

NOTE: you can connect back to the Remote VPN Workstation and use Nmap on the desktop to generate more traffic targeting the internal 198.19.20.0/24 subnet if you would like to explore more.

In this test case we created a custom security event to notify us if Stealthwatch ever sees internal Telnet traffic an alarm will fire as indicated above.

Telnet is an unsecure protocol with clear text traffic. It should never be used. This is just an example of how to create custom security events within Stealthwatch

Summary

Within this testing plan you learned:

- How to create a Custom Watchlist for Telnet communications
- How to simulate telnet traffic from the network
- How to access the Visibility Assessment
- Review the DNS Observation

Encrypted Traffic Analytics (ETA)

Business Objectives

The percentage of encrypted traffic over the public Internet has been increasing each year since the IP protocol began to support cryptography. The use of Internet Protocol (IP) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) cryptography grew 90 percent from 2015 to 2016.

Industry analysts from Gartner predict that more than 80 percent of all web traffic will be encrypted by 2019. Encrypted traffic hides possible threats to a network. Until recently, there was no way to analyze encrypted traffic without decrypting it; making it difficult to effectively monitor networks for threats. Cisco Encrypted Traffic Analytics addresses this problem by producing new telemetry data specifically derived from SSL / TLS connections. This data is then exported to a Stealthwatch Flow Collector where it is processed and stitched with connection data to provide new insights into network communications.

Using the Encrypted Traffic Analytics (ETA) technology, Stealthwatch detects malware in encrypted traffic without decryption by collecting network telemetry from Cisco IOS-XE devices including routers, switches, and Wireless LAN Controllers. Stealthwatch uses this data along with advanced entity modeling and multilayer machine learning to improve the fidelity of malware detection in encrypted traffic. These new techniques also use the Talos global threat map to identify and correlate known global threats to the local environment.

Requirements

Visit <http://www.cisco.com/go/eta> for an overview on ETA, how to enable it, and how to get started.

The Stealthwatch system configuration requirements are:

- Stealthwatch Cloud Portal
- ETA capable device
- Version 4 or newer of the Stealthwatch Cloud sensor

ETA capable platforms include the following devices (routers, switches or wireless LAN controllers running Cisco IOS-XE version 16.6 or later with a security feature license):

- Cisco Catalyst 9300 series switch
- ASR 1000 Series Aggregation Services Routers
- 4000 Series Integrated Services Routers
- Cloud Services Router 1000V Series

- Stealthwatch Flow Sensor v7.1 or later

Review Vulnerable Transport Alert

Stealthwatch cloud includes built-in alerts using Enhanced NetFlow + Cognitive (ETA) to perform additional detections.

1. Click on alerts in the main menu. There should be an auto generated alert for a machine using TLS1.0 which is important as browsers will soon stop supporting this version of TLS.
2. Select the **Vulnerable Transport Protocol Alert** which uses ETA for detection.

Figure 82. ETA Based Alert

The screenshot shows a detailed view of a 'Vulnerable Transport Security Protocol' alert. At the top, there's a red exclamation mark icon and the text 'Vulnerable Transport Security Protocol -'. To the right, it shows the IP address '198.19.20.51 -' with a red exclamation mark. Below this, the alert status is 'Open'.

Status: Open

ID: 135

Description: Device was observed using an insecure SSL/TLS protocol version. This alert is part of Encrypted Traffic Analytics capabilities.

Updated: Dec 6, 2019 2:52:18 PM

Created: Dec 6, 2019 1:52:20 PM

IPs at the time of alert: 198.19.20.51

Assignee: Nobody

Tags:

A blue callout box contains the text: 'After reviewing an alert, closing it will let the rest of your team know it's been resolved. In addition, closing alerts sends important feedback.' with a close button 'x'.

Close Alert

Supporting Observations

Insecure Transport Protocol Observation

Device was observed using an insecure transport protocol. This observation uses information from Enhanced NetFlow.

Time	Device	Device	port	Transport version
12/6/19 2:52 PM	198.19.20.51	23.21.44.116	443 (https)	TLS 1.0
12/6/19 2:51 PM	198.19.20.51	208.90.58.6	443 (https)	TLS 1.0
12/6/19 2:40 PM	198.19.20.51	208.90.58.6	443 (https)	TLS 1.0

Crypto audit to enforce authorized encryption standards

- Many organizations are interested in tools and techniques that can be used to better ensure the security of data and applications that they use. Using the ETA data and the Stealthwatch Crypto Audit users can examine and report on cryptographic protocols and parameters used to establish encrypted communications to one or more hosts.
- Conduct and leverage a flow search to detect which encryption suites are being used on the network. Algorithms such as SHA-1 and RC4, as well as SSLv3 protocol are no longer considered secure. These algorithms and protocols are considered obsolete and are being retired by Microsoft and Google. They are being replaced by AES, RSA and SHA-3, and others.

Review Encrypted Traffic Query

Similar to the flow query we did earlier, Stealthwatch cloud includes a query to see what version of encryption are being used on the network.

- Click on **Models** in the main menu, then select **Encrypted Traffic**. Encryption data for the past 24 day will be displayed.

Figure 83. Encryption Query

The screenshot shows a table titled "Encrypted Traffic" with the following data:

Time	Remote				Encryption				
	IP	Port	IP	Port	Protocol	Key Exchange	Key Length	Algorithm	MAC
12/6/19 3:49 PM	198.19.20.137	46670	34.249.146.196	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.137	46648	34.249.146.196	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.137	33620	52.51.131.41	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.143	40918	107.22.247.3	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.143	40916	107.22.247.3	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.143	60184	52.217.32.118	443 (https)	TLS 1.2	ECDHE_RSA		AES_128_GCM	SHA256
12/6/19 3:49 PM	198.19.20.143	36334	107.22.217.211	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.143	60178	52.217.32.118	443 (https)	TLS 1.2	ECDHE_RSA		AES_128_GCM	SHA256
12/6/19 3:49 PM	198.19.20.143	42958	107.22.210.176	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.143	40908	107.22.247.3	443 (https)	TLS 1.2	ECDHE_RSA		AES_256_GCM	SHA384
12/6/19 3:49 PM	198.19.20.143	60172	52.217.32.118	443 (https)	TLS 1.2	ECDHE_RSA		AES_128_GCM	SHA256

2. Select **Active Filters** to expand the list of security filter options. Pick a few to see if they are present in this network. We already know TLS1.0 is being used, select **TLS 1.3** in the protocol field to see what websites are using that.

Figure 84. Encryption Filter Options

The screenshot shows the 'Encryption Filter Options' page. At the top, there is a search bar labeled 'active filters'. Below it, there are three sections for filtering by IP, Port, and encryption properties. The 'IP' section has fields for 'IP' and 'Remote IP'. The 'Port' section has fields for 'Port' and 'Remote Port'. The 'Encryption Properties' section includes fields for 'Protocol' (dropdown), 'Algorithm' (dropdown), 'Key Exchange' (dropdown), 'Key Length' (dropdown with 'Min' and 'Max' buttons), and 'MAC' (dropdown). At the bottom, there are date and time selection fields for 'Start Date' (2019-12-06) and 'End Date' (2019-12-07), and time selection fields for 'Start Time' (00:00) and 'End Time' (00:00). A blue 'Update' button is located at the bottom left of the form area.

Q active filters

Filter by a list of IPs. Use "-" to exclude an IP (e.g. "10.0.0.1, 10.0.1.0/24, -10.0.1.7").

IP IP, host ...

Remote IP IP, host, ...

Filter by a list of ports or port ranges. Use "-" to exclude a port. (e.g. "22-25, 80, -443").

Port port or range of ports

Remote Port port or range of ports

Filter by encryption properties

Protocol

Algorithm

MAC All

Enter a start date/time and end date/time for the search. Longer time ranges will take longer to load.

Start Date 2019-12-06

End Date 2019-12-07

Start Time 00:00

End Time 00:00

Update

Appendix

Understanding NetFlow & IPFIX

Business Objectives

The primary data source of Stealthwatch is NetFlow. NetFlow is network traffic metadata that most current routers, switches and firewalls generate. This gives the administrator the ability to have 1-to-1 conversational visibility throughout a network. The conversations can be east-to-west client-to-client, or north-to-south client to Internet communications.

Test Drive Objectives

To fully understand Stealthwatch capabilities, you need a basic understanding of the different types of NetFlow, the devices that support NetFlow and the metadata that is contained in a NetFlow template. After this test drive, you will be able to articulate the different versions of NetFlow, types of supported NetFlow-capable devices and perform a basic Packet Capture (PCAP) analysis of NetFlow traffic.

Test Drive Requirements

The Stealthwatch system configuration minimum requirements are:

- NetFlow or IPFIX records that meet the minimum fields defined in this lab
- Visibility of all host-to-host traffic from the core, distribution, or access layer
- Any Stealthwatch version

Test Drive Outline

Someone from the NetOps team has called in and stated they have configured NetFlow on the router and switches in your infrastructure. You are looking at the Stealthwatch Management Console and don't see flows coming into the Flow Collector from the Security Insight Dashboard. You need to do some basic NetFlow troubleshooting by conducting a full packet capture on the Flow Collector and viewing the capture in Wireshark. You are provided NetFlow PCAPs in dCloud during this lab for analysis.

Lab: Understanding NetFlow

What is NetFlow?

NetFlow is a feature that was originally introduced on Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.

What are the various kinds of NetFlow?

Most enterprise class networking devices today support some variant of NetFlow. These can go by different names, so you may run across one or more of these in client environments:

- FNF (Flexible NetFlow)
- NSEL (NetFlow Security Event Logging)
- IPFIX (IP Flow Information Export)
- TNF (Traditional NetFlow)
- FlowCache
- NetFlow-lite Phase 1
- NetFlow-lite Phase 2
- AVC (Application Visibility and Control)
- NBAR2 (Network-Based Application Recognition)
- sFlow (Sampled Flow)

These all differ in various ways, and some Cisco devices can export NBAR2 as part of AVC which can provide extra application information to assist in investigations with Stealthwatch.

What NetFlow information is Stealthwatch expecting to see?

Stealthwatch expects specific NetFlow fields to be passed for it to properly analyze network traffic. Together, these fields comprise the NetFlow template.

The most common issue experienced when setting up Stealthwatch is invalid template errors. On most devices, you will be able to modify the NetFlow fields sent to Stealthwatch to receive the proper template information. For those devices that cannot send the proper template information, you will need to either rely on the NetFlow generated by other devices or install a device like a Stealthwatch Flow Sensor to generate NetFlow that Stealthwatch can interpret for you.

The **Required** and **Optional** NetFlow fields that Stealthwatch ingests are:

Description	Required or Optional?	Notes
match ipv4 protocol	Required	Key field
match ipv4 source address	Required	Key field
match ipv4 destination address	Required	Key field
match transport source-port	Required	Key field
match transport destination-port	Required	Key field
match interface input	Required	Key field
match ipv4 tos	Required	Key field
collect interface output	Required	Key field
collect counter bytes	Required	Key field
collect counter packets	Required	Key field
collect timestamp sys-uptime first	Required	For calculating duration
collect timestamp sys-uptime last	Required	For calculating duration
collect routing next-hop address ipv4	Optional	Used for closest interface determination
collect ipv4 dscp	Optional	Used for closest QoS monitoring
collect ipv4 ttl minimum	Optional	Used for to understand the path of flow
collect ipv4 ttl maximum	Optional	Used for to understand the path of flow
collect transport tcp flags	Optional	Used for reporting on TCP flags

collect routing destination AS	Optional	Used for AS reporting
collect application name	Optional	Used to capture layer 7 application name when NBAR2 is being used
collect application http host	Optional	Used to capture URL information when AVC is being used

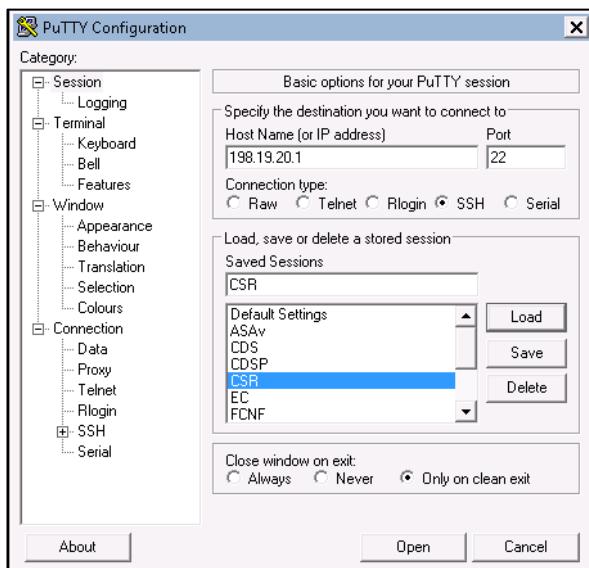
Steps to enable flow

1. Create a [Flow Record](#)
2. Configure the [Exporter](#)
3. Configure the [Monitor](#)
4. Configure the [Interface\(s\)](#)

View flow configurations from the CSR Router

1. Open Putty, load the CSR configuration and open the session as shown below:

Figure 85. Putty Configuration



2. The session will load with the username admin
 - a. Insert the password of **C1sco12345**
3. Use the following command to view the interfaces flow is being exported from

- a. [show flow interface](#)
4. You should see the output as shown:

Figure 86. Show flow interface

```
CSR#show flow interface
Interface GigabitEthernet1
  FNF: monitor:          IPv4_NETFLOW
        direction:       Input
        traffic(ip):    on
Interface GigabitEthernet2
  FNF: monitor:          IPv4_NETFLOW
        direction:       Input
        traffic(ip):    on
CSR#
```

Note: The direction of the flow: [Input](#). When enabling flow, it is best practice to enable flow on the interface in the ingress direction

5. View the flow exporter with the following command:
 - a. [show run flow exporter](#)
6. The output should be the same as below

Figure 87. Show flow exporter

```
CSR#show run flow exporter
Current configuration:
!
flow exporter NETFLOW_TO_STEALTHWATCH
  description Export NetFlow to SW
  destination 198.19.20.139
  transport udp 2055
  template data timeout 30
  option interface-table
!
CSR#
```

7. Issue the following command:
 - a. [show run flow monitor](#)
8. The output should be the same as below:

Figure 88. Show flow monitor

```
CSR#show run flow monitor
Current configuration:
!
flow monitor IPv4_NETFLOW
  exporter NETFLOW_TO_STEALTHWATCH
  cache timeout active 60
  record STEALTHWATCH_FLOW_RECORD
!
CSR#
```

Note: The cache timeout on Cisco devices be default is [30 minutes](#). Stealthwatch needs the cache active timeout to be 1 minute or 60 seconds.

9. Issue the command

a. [show run flow record](#)

10. Take note of the output shown below:

Figure 89. Show flow record

```
CSR#show run flow record
Current configuration:
!
flow record STEALTHWATCH_FLOW_RECORD
  description NetFlow record for SW
    match ipv4 tos
    match ipv4 source address
    match ipv4 destination address
    match transport destination-port
    match transport source-port
    match interface input
    match ipv4 protocol
      collect routing source as
      collect routing destination as
      collect routing next-hop address ipv4
      collect ipv4 dscp
      collect ipv4 id
      collect ipv4 source prefix
      collect ipv4 source mask
      collect ipv4 destination mask
      collect ipv4 ttl minimum
      collect ipv4 ttl maximum
      collect transport tcp flags
      collect interface output
      collect counter bytes
      collect counter packets
      collect timestamp sys-uptime first
      collect timestamp sys-uptime last
!
CSR#
```

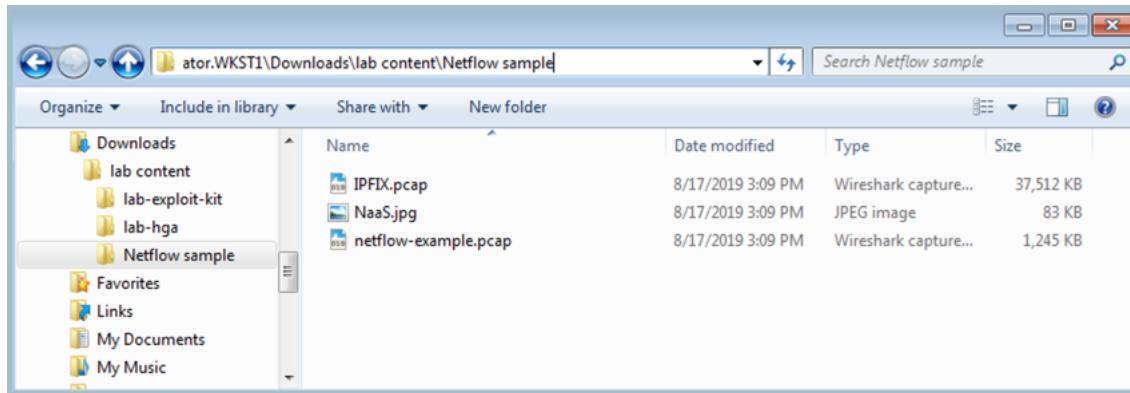
Note: The highlighted match and collect statements above are required fields in Stealthwatch. The other fields are optional to collect additional data.

Review this tool that was built by a Cisco engineering on sample NetFlow configurations on a per devices bases: <https://configurenflow.info/>. This is a good resource when having NetFlow enabled within your environment.

Reviewing a NetFlow Packet Capture

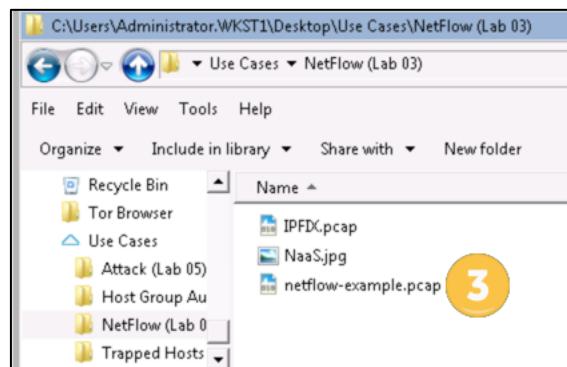
1. From Wkst1, open the [Downloads > lab content](#) from Windows Explorer.
2. Open the [NetFlow sample](#) folder

Figure 90. NetFlow sample pcaps



3. Open the [netflow-example.pcap](#) file
 - a. Note: If a Wireshark update window appears, select skip this version.

Figure 91. NetFlow-example.pcap file



4. Select the first packet from the capture

Figure 92. Wireshark packet listing of **netflow-example.pcap**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
2	1.945376	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
3	32.707583	198.18.133.36	198.18.133.137	CFLow	1220	total: 24 (v5) flows
4	42.742817	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
5	45.897316	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
6	45.897433	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
7	47.741774	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
8	47.741984	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
9	47.742047	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
10	47.742251	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
11	47.742454	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
12	50.742417	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
13	53.766295	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows
14	53.766389	198.18.133.36	198.18.133.137	CFLow	1508	total: 30 (v5) flows

5. In the middle section of Wireshark, click the + next to Cisco NetFlow/IPFIX

Figure 93. Packet details of netflow-example.pcap

```

[+] Frame 1: 1508 bytes on wire (12064 bits), 1508 bytes captured (12064 bits)
  [+] Linux cooked capture
  [+] Internet Protocol Version 4, Src: 198.18.133.36, Dst: 198.18.133.137
  [+] User Datagram Protocol, Src Port: 50432, Dst Port: 2055
  [+] Cisco NetFlow/IPFIX
    - Version: 5
    - Count: 30
    - SysUptime: 171.957000000 seconds
    - Timestamp: May 3, 2017 01:49:00.0000000302 Eastern Daylight Time
    - FlowSequence: 124
    - EngineType: RP (0)
    - EngineId: 158
    - 00... .... .... = SamplingMode: No sampling mode configured (0)
    - ..00 0000 0000 0000 = SampleRate: 0
    [+] pdu 1/30
    [+] pdu 2/30
    [+] pdu 3/30
    [+] pdu 4/30
    [+] pdu 5/30
    [+] pdu 6/30
    [+] pdu 7/30
    [+] pdu 8/30
    [+] pdu 9/30
  
```

Click to expand one of the PDU's as shown above. PDU is short for Protocol Data Unit. The term used to describe data as it moves from one layer of the OSI model to another. In this reference, PDU is often used synonymously with packet.

6. Compare the fields in the pdu to the figure below.

Figure 94. Expanded PDU

```

+ Frame 1: 1508 bytes on wire (12064 bits), 1508 bytes captured (12064 bits)
+ Linux cooked capture
+ Internet Protocol Version 4, Src: 198.18.133.36, Dst: 198.18.133.137
+ User Datagram Protocol, Src Port: 50432, Dst Port: 2055
+ Cisco NetFlow/IPFIX
  - Version: 5
  - Count: 5
  - SysUptime: 171.957000000 seconds
  - Timestamp: May 3, 2017 01:49:00.0000000302 Eastern Daylight Time
  - FlowSequence: 124
  - EngineType: RP (0)
  - EngineID: 158
  - 00. .... .... = SamplingMode: No sampling mode configured (0)
  - ..00 0000 0000 0000 = SampleRate: 0
+ pdu 1/30
  - SrcAddr: 198.18.133.137 match ipv4 source address - required - key field
  - DstAddr: 198.18.133.36 match ipv4 destination address - required - key field
  - NextHop: 0.0.0.0 collect routing next-hop address - optional - used for closest interface determination
  - InputInt: 0 match interface input - required key field
  - OutputInt: 0 collect interface output - required - key field
  - Packets: 3 collect counter packets - required - key field
  - Octets: 498 collect counter bytes - required - key field
  - [Duration: 2.379000000 seconds]
    - StartTime: 123.638000000 seconds collect timestamp sys-uptime first - required - key field
    - EndTime: 126.017000000 seconds collect timestamp sys-uptime last - required - key field
  - SrcPort: 443 match transport source-port - required - key field
  - DstPort: 54836 match transport destination-port - required - key field
  - Padding: 00
  - TCP Flags: 0x19 collect transport tcp flags - optional - used for closest interface determination
  - Protocol: TCP (6) match ipv4 protocol - required - key field
  - IP TOS: 0x00 match ipv4 tos - required - key field
  - SrcAS: 0
  - DstAS: 0 collect routing destination as - optional - used for closest interface determination
  - SrcMask: 0 (prefix: 198.18.133.137/32)
  - DstMask: 0 (prefix: 198.18.133.36/32)
  - Padding: 0000
+ pdu 2/30

```

You may need to do a similar analysis of a packet if Stealthwatch is giving invalid template errors for a device, and the configuration looks accurate.

If any NetFlow fields are missing, like the source IP, time stamps, or byte counters that Stealthwatch requires, you will need to have the NetFlow record on the source exporters adjusted to contain the minimum required fields.

Summary

In this lab you learned:

- That Stealthwatch uses NetFlow as its primary data source
- The different types of NetFlow
- Which NetFlow fields are required versus optional
- How to decode a NetFlow packet with Wireshark
- How to decode an IPFIX packet with Wireshark

End of Lab: Please pause here.

